

EXHIBIT 1

Redacted Version of Document
Sought to be Sealed

Message

From: Parisa Tabriz [parisa@google.com]
Sent: 2/11/2015 6:57:06 PM
To: Chris Palmer [palmer@google.com]
CC: Adrienne Porter Felt [felt@google.com]
Subject: Re: Incognito-fest 2015

On Wed, Feb 11, 2015 at 10:52 AM, Chris Palmer <palmer@google.com> wrote:

On Wed, Feb 11, 2015 at 4:41 AM, Adrienne Porter Felt <felt@google.com> wrote:

> Second question. Is Incognito something our team wants to take on? (Palmer,
> in Q2 or Q3?) It would take attention and focus away from HTTPS but OTOH it
> is also something I know we all care about. Or should we focus on trying to
> poke the privacy team into action?

1. Sure, I can give a brief briefing. What is the best format?
Document, slides, in-person chat, a CL that has +0 lines and -15000?
:)

2a. I'm not sure we should take it on. It's radioactive: In its
current form, it is effectively a lie; in its fixed form (rebranded,
clarified) it will be a huge negative press cycle like Master Password
was (most people drunkenly screeching; Kevin Poulsen being the lone
sane voice); in its genericized form ([REDACTED]
[REDACTED]) people will
think we killed it unceremoniously and then it will be 100%
screeching.

I'd prefer our team does not take this on and Chrome Privacy steps up.

2b. If we don't take it on, it will fester and perhaps metastasize,
and we will feel like we were derelict in our duty.

I think we should help Chrome Privacy step up.

2c. Does Privacy team realize they have dropped the ball? I.e. if we
try to take it on, will they push back thinking it's still theirs? Or,
can we get them on board with our plan and then get them to act on it,
solving (2a)?

Which Privacy Team are we talking about? I consider Chrome Privacy distinct from "Privacy Team" (where
Garth comes from)...

EXHIBIT 3

Redacted Version of Document
Sought to be Sealed

Message

From: palmer@google.com [palmer@google.com]
Sent: 7/11/2018 4:44:17 PM
To: palmer@google.com; jyasskin@google.com; estark@google.com; kenrb@google.com; ellyjones@google.com; agl@google.com; sleevi@google.com
Subject: AAAA952KuYI-IULXO2v58wc

- **palmer@google.com** 2018-07-11T16:44:17.423Z

There's some interest in [REDACTED] again

- **palmer@google.com** 2018-07-11T16:44:36.620Z

Mozilla and IPT 2 have everyone what we can do (which is good)

- **Updated on** 2018-07-11T16:52:30.089Z

Mozilla and IPT 2 have everyone wondering what we can do (which is good)

- **palmer@google.com** 2018-07-11T16:44:45.067Z

but I remain not on-board with [REDACTED] per se

- **palmer@google.com** 2018-07-11T16:44:54.465Z

what do other people think?

- **jyasskin@google.com** 2018-07-11T16:45:08.462Z

Also <https://brave.com/tor-tabs-beta/>.

- <https://brave.com/tor-tabs-beta/>

- **Updated on** 2018-07-11T16:52:18.703Z

Also <https://brave.com/tor-tabs-beta/>.

- <https://brave.com/tor-tabs-beta/>

- **estark@google.com** 2018-07-11T16:45:10.704Z

"Mozilla and IPT 2 have everyone what we can do" <-- missing a word?

- **kenrb@google.com** 2018-07-11T16:49:13.034Z

the question is whether we should consider trying to add web anonymization to Incognito?

- **estark@google.com** 2018-07-11T16:49:30.440Z

- **estark@google.com** 2018-07-11T16:49:38.983Z

and is basically orthogonal?

- **palmer@google.com** 2018-07-11T16:51:51.768Z

Oh, sorry: *wondering* what we can do

- **palmer@google.com** 2018-07-11T16:52:12.512Z

@Emily Stark Yes. But, people are just brainstorming.

- **estark@google.com** 2018-07-11T16:53:06.993Z

@Mike West has lots of Thoughts on the ITP stuff, have you seen any of his docs/brainstorms already?

- **palmer@google.com** 2018-07-11T16:53:14.634Z

1 idea was to [REDACTED] (!!!). I was like, no.

- **kenrb@google.com** 2018-07-11T16:53:23.823Z

- **palmer@google.com** 2018-07-11T16:53:32.557Z

Yeah I joined the [REDACTED] list, if that's what you mean @Emily Stark

- **palmer@google.com** 2018-07-11T16:54:15.470Z

a fear is that too-good tracking prevention will just escalate the arms race and we'll end up in a Fingerprinting Nightmare World

- **ellyjones@google.com** 2018-07-11T16:54:16.981Z

We looked at this for Chrome OS many years ago also

- **palmer@google.com** 2018-07-11T16:54:20.311Z

yeah

- **estark@google.com** 2018-07-11T16:54:25.686Z

in a former life I worked on a project to bundle a node in every webpage ☺

- **ellyjones@google.com** 2018-07-11T16:54:31.290Z

and the [REDACTED] people hard passed on the idea of shipping a [REDACTED] node on each chromebook - it would have demolished their infra

- **ellyjones@google.com** 2018-07-11T16:54:49.786Z

(this was in like 2011 so maybe things have changed)

- **ellyjones@google.com** 2018-07-11T16:55:03.495Z

I know Sleevi has strong feelings about [REDACTED]

- **estark@google.com** 2018-07-11T16:55:45.126Z

@Chris Palmer I also fear the Prompt On Every Subresource For Every Webpage Nightmare World

- **kenrb@google.com** 2018-07-11T16:56:09.079Z

@Chris Palmer but maybe we can reduce fingerprinting vectors to the point where few people are individually distinguishable

- **ellyjones@google.com** 2018-07-11T16:56:19.715Z

"This website would like to load an image. [Allow] [Deny]"

- **agl@google.com** 2018-07-11T16:58:17.233Z

Clearly the answer is for the whole world to use AMP, then we can expose the AMP cache via a Private Information Retrieval protocol and disable Javascript when rendering.

- **palmer@google.com** 2018-07-11T16:59:15.671Z

that is... wow

- **palmer@google.com** 2018-07-11T16:59:25.640Z

If I weren't already sitting down, I'd need to sit down

- **jyasskin@google.com** 2018-07-11T17:00:45.654Z

I assume everyone's seen <https://www.blaseur.com/papers/www18privatebrowsing.pdf>? (Thanks @Martin Shelton)

- <https://www.blaseur.com/papers/www18privatebrowsing.pdf>

- **palmer@google.com** 2018-07-11T17:01:04.761Z

yep, I am waving it in front of people

- **palmer@google.com** 2018-07-11T17:01:36.786Z

I am going to get back on my old shit of yelling that we need to stop calling it Incognito and stop using a Spy Guy icon

- **palmer@google.com** 2018-07-11T17:01:40.468Z

Temporary Mode

- **palmer@google.com** 2018-07-11T17:02:27.381Z

although that paper does note that people were least confused by Chrome's disclosure (their word for the disclaimer/explainer language)

- **palmer@google.com** 2018-07-11T17:02:54.443Z

Incognito: Voted Least Confusing Private Mode, 2018

- **ellyjones@google.com** 2018-07-11T17:04:37.562Z

good news palmer

- **ellyjones@google.com** 2018-07-11T17:04:47.313Z

we're working on a Dark Mode for Mac Chrome that will probably look quite a bit like incognito

- **kenrb@google.com** 2018-07-11T17:05:32.947Z

call it 'Dark Web Mode'

- **ellyjones@google.com** 2018-07-11T17:05:50.778Z

I love it

- **palmer@google.com** 2018-07-11T17:06:44.351Z

sob

- **kenrb@google.com** 2018-07-11T17:07:04.006Z

@Chris Palmer I know the 'incognito' war was waged and lost years ago, but do you remember why? It has always been a misleading name

- **palmer@google.com** 2018-07-11T17:07:22.790Z

Just as long as we don't get a Dark Intellectual Web Mode

(<https://www.nytimes.com/2018/05/08/opinion/intellectual-dark-web.html>)

- <https://www.nytimes.com/2018/05/08/opinion/intellectual-dark-web.html>

- **ellyjones@google.com** 2018-07-11T17:07:40.746Z

regardless of the name, the icon should always have been http://simpsons.wikia.com/wiki/Guy_Incognito

- http://simpsons.wikia.com/wiki/Guy_Incognito

- **ellyjones@google.com** 2018-07-11T17:07:49.327Z

which also accurately conveys the level of privacy it provides I think

- **palmer@google.com** 2018-07-11T17:08:13.654Z

@Ken Buchanan They didn't believe me that people would get confused; and they were still loving the Aw, Snap!/i18n-resistant whimsy thing

- **palmer@google.com** 2018-07-11T17:08:17.227Z

Maybe now is the time

- **kenrb@google.com** 2018-07-11T17:08:37.081Z

I see

- **palmer@google.com** 2018-07-11T17:08:38.747Z

now that we have results from, among others, a person we offered an Enamel job to (Sascha Fahl, co-author)

- **kenrb@google.com** 2018-07-11T17:09:13.964Z

"We have this wall of text explaining to people that incognito doesn't mean unrecognizable, when we use it"

- **sleevi@google.com** 2018-07-11T20:03:52.557Z

Yes, Eric Roman has similarly Strong Feelings about [REDACTED]. In theory, I'm not opposed to [REDACTED]
[REDACTED] is that it's
largely un(der?)staffed. Between [REDACTED], things just get... really weird and unpredictable. I
mean, same as Android, just more weird. [REDACTED]
[REDACTED].

EXHIBIT 4

Redacted Version of Document
Sought to be Sealed

Message

From: Rachel Popkin (Google Docs) [comments-noreply@docs.google.com]
Sent: 12/10/2018 9:33:08 PM
To: mardini@google.com
Subject: Synthesized Themes for Browser 6 Pager

Rachel Popkin added comments to Synthesized Themes for Browser 6 Pager

New

2 comments

New

Comments



Adrienne Porter Felt

We have to stop thinking about privacy as a bit flip within Chrome and instead think of it as a core part of our product. We have to re-think flows from the beginning, making it transparent to users when and how their data is being shared and then give them the control to either edit or remove that data. We have to be able to do this for our first party relationship with Google, through third-party relationships with websites, and within the complexity of shared-device scenarios.

something we need to decide: how far do we want to go with this?

do we want to stop opting people in to [REDACTED] by default? do we want to build federated analysis with [REDACTED]



Parisa Tabriz

I think we need to understand what problems we're solving first. For example, even if we could design and publish a provably privacy-preserving system to do ad remarketing, I'm not sure if that makes it any less creepy to users or will mean Apple criticizes us any less.

I'd love to be challenged on this, but I don't think we get criticism because [REDACTED] is opt-out, or even got any criticism when we made the opt-in-to-opt-out change. My guess is because (1) most users don't care about/understand this level of detail (2) users that do care think the tradeoff and change was reasonable.

From my view, sync/identity/privacy+security-settings are just way too complicated, and users can't make any reasoned tradeoffs for themselves without more help. Also, incognito is a confusing mess that also doesn't have high user awareness, and all of this makes situations where people use Chrome in shared settings dangerous (w.r.t. privacy). If we could materially address some of these problems, I'd be pretty happy.



AbdelKarim Mardini

I don't think [REDACTED] and the likes are the issue. If we're talking about user perception/feelings, there is a clear PR/narrative issue that needs concerted x-functional effort to fix regarding privacy, in-product as well as off-product. It's also not a Chrome issue per se but a Google issue overall and Chrome is collateral damage.



Rachel Popkin

I just caught up with bgalbs on potassium's 2 year plan, and I'm newly worried about history sync. Let's discuss!

ReplyOpen



AbdelKarim Mardini

who remix and create content

The mental model I had been using here is the creation of public "Play Lists" about topics (well, Reading Lists", I guess) that are analogous to users who create public Deezer/Spotify Plalists, or public maps with interesting stuff on it, ...etc. Is this what you mean by remixing?



Rachel Popkin

I think remix involves changing or layering on something new - but maybe curation is part of that! I love the idea of play lists for the web on certain topics.

ReplyOpen

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

You have received this email because you are a participant in the updated discussion threads. Change what Google Docs sends you. You can not reply to this email.



EXHIBIT 5

Redacted Version of Document
Sought to be Sealed

Message

From: Lorraine Twohill [lorraine@google.com]
Sent: 1/29/2021 3:30:31 AM
To: Sundar Pichai [sundar@google.com]; Rahul Roy-Chowdhury [rahulrc@google.com]; Jen Fitzpatrick [jen@google.com]; Luiz André Barroso [luiz@google.com]
Subject: Today is Data Privacy day...so please read!

Hi folks,

As today is International Data Privacy Day (check out our [homepage](#)), and Privacy has been on my mind, as well as all of yours for some time, I wanted to share some thoughts. It has been almost 11 years since I first spoke at Exec Circle (and Ben listened!) about User Trust and needing a Google Account with controls. And 7 years since I did the User Trust tgif. I have been doing a lot of thinking (and asking!) over the years. And we have made a lot of progress but our challenges are even greater. We need more velocity! So, since I know you all agree, and I know Sundar that you have been thinking about this too, I wanted to share my random thoughts here, as hopefully somewhat useful and actionable. And yes there will be reasons why a lot of this is hard, but we are at our best when solving really hard problems! And then just maybe we could get to this vision that we put together just over a year ago,

With the greatest of respect, and apologies in advance for my ramblings...

L.

What I think we need:

- 1.
2. Much more visible comms on and off product
- 3.
- 4.
5. Privacy as a feature/products making meaningful change
- 6.
- 7.
8. Definitive progress in ads, including showing that we are ok losing out too
- 9.
- 10.
11. Owning our absolute strength in security
- 12.
- 13.
14. Other random ideas that could help

1. Much more visible comms on and off product

In 2020, we sent over [REDACTED] users to our privacy check ups and [REDACTED] to our security check up from our homepage and promo efforts. But it feels completely separate from those *moments of truth* when a user is in-product and needs our help. What if we:

•

•

[REDACTED] There's a number of moments in product where we already use the shield and messaging to signal

privacy and security protections (e.g., “only you can see this” for Google Account related queries in Search and in My Activity). But we need to accelerate implementation across PAs so it shows up in the products people use every day.

-
-
- **Increase user facing reassurances in-product:** No more unexplained features or cross-product data usage that freaks a user out. We know that a feature can trigger user concern over how their data is being used and why (particularly x-app). Increase investment and prioritize [REDACTED] to provide users with helpful transparency, education, and access to their controls in these moments.
-
-
- **Explain ourselves much, much better. And do that everywhere.** This is not new work but is a compelling way of talking about the data we have, 3 types of data, stuff you save, stuff you do (your activities) and stuff we use for ads (much smaller). If we did this well, everywhere, including in your Google Account, it would help a lot.
-
-
- **Move our promo real estate to the TOP of the screen in mobile.** Instead of push-up promos, move them to the top of the screen so they are unmissable. Instagram P&S promos are at the top of the screen. Twitter’s promos are overlays. At the bottom of the screen, ours don’t have the same gravity and visibility, making our P&S messages feel unimportant/optional. By adding some friction we will increase engagement and demonstrate to users and KOFs that privacy and security are a top priority.
-
- **Establish GSEC(Google Safety Engineering Center) in the US.** Building on the successful launch of GSEC Munich (and GSEC Dublin) let’s identify key offices where we have strong privacy efforts (e.g. Cambridge for Chrome) and establish GSEC in the US as a key part of our KOF outreach efforts.

2. Privacy as a feature/products making meaningful change

We need more products built upon our privacy north star that PDPO has been championing. Our collaboration with Pay is a good example of how a product can build privacy and security right into the product (‘A safer way to pay’). But there is more that is needed to ensure that across the company we live up to the new privacy principles and develop consistent, scalable privacy features that bring those principles to life. Could we start with:

Giving users more transparency and control over their data

-
- [REDACTED]
- [REDACTED]
-
-
- [REDACTED]
- [REDACTED]
-
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

Creating more visible, ownable privacy products and brands:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

3. Make faster and more demonstrable progress on ads

Users point to our ads as THE reason why they can't trust Google and why they think we sell their personal information to 3rd parties. While we have made great progress with things like our recent Privacy Sandbox announcement there is more we need to do here faster. We could start with:

- [REDACTED]
- **Focus on where we think the long term is in Ads.** [REDACTED]

- [REDACTED]
- **Improve Ads Settings/make this a much bigger deal:** [REDACTED]

[REDACTED]. This [page](#) is decent, we need to tell people about it in product and link to it, and we need to promote it and also make it better.

- [REDACTED]
- [REDACTED]

- **Making Mute this Ad a more valuable property.** Every ad has 'mute this ad' but the current experience is limited and does not allow us to tell our story to our users. [REDACTED]

-
-
- **Accelerating potential changes in ad retargeting.** [REDACTED]

-
-
-
- **Further accelerate Privacy Sandbox efforts:** As part of the Privacy Sandbox effort to replace 3P cookies in Chrome, [REDACTED]

-
-
- **Push for Privacy Norms faster:** In parallel to Privacy Sandbox, Ads is working to get internal alignment on a [REDACTED]

-
-
- **Increase velocity around Experiments:** Beyond the Privacy Sandbox and Privacy Norms efforts, there are also user experiments being conducted in Ads, such as one that [REDACTED]

-
-
- **Explore tagging ads that preserve privacy.** Introduce a [REDACTED] (anonymized). Make this work across all surfaces, building from Chrome. Brand these ads!

-
-
- **Mythbust Data Selling:** [REDACTED] of users believe we sell their data. We need to do more to communicate to them **in-product** that their data is never sold and never shared without their permission.

4. Owning our absolute strength in security

We do a lot to keep people safe across Chrome, Android, Gmail and your Google account but people have no idea. We keep lots of KOFs safe and governments, but do we tell them? Users see privacy and security as two sides of the same coin so our leadership here is a huge opportunity. Could we:

-
- **Develop a bolder Security claim.** What is the equivalent of "Never sell our users' personal information to anyone" for Security. Our current version ("Build the strongest security technologies into our products") does

not seem bold enough. [REDACTED]

•

•

• **Humanize our Security efforts:** [REDACTED]

•

•

• **Add helpful security tips to every security email.** The emails we send to verify when users have signed into a new device are the most frequent email we send - super high volume and frequency of impressions - so much so that there are memes online about Google Security detecting anything suspicious

•

•

• **More visibly surface security benefits in user comms.** Remind users of all the occasions where we have their back. One of the reasons MSFT is scoring well on security is that you have to consciously update versions, install virus protections, etc. In our case we do a lot of that invisibly (in Chrome/Chrome OS/Android/Play Protect/Gmail). For example we could: [REDACTED]

•

•

• **Treat users like VIPs when security issues arise:** Beyond communicating how we're activating our 'automatic' protections, such as spam protections in Gmail, [REDACTED]

•

•

• **Incentivize users to use our security features.** Put our money where our mouth is. Show that we care about our users' safety so much we will [REDACTED]

5. Other random ideas that could help

These are various other areas we could invest in that would help. We should think about:

•

• [REDACTED]

•

•

• [REDACTED]

•

- Developing an [REDACTED]

If you got this far, thank you for reading!

Your privacy obsessed pal...

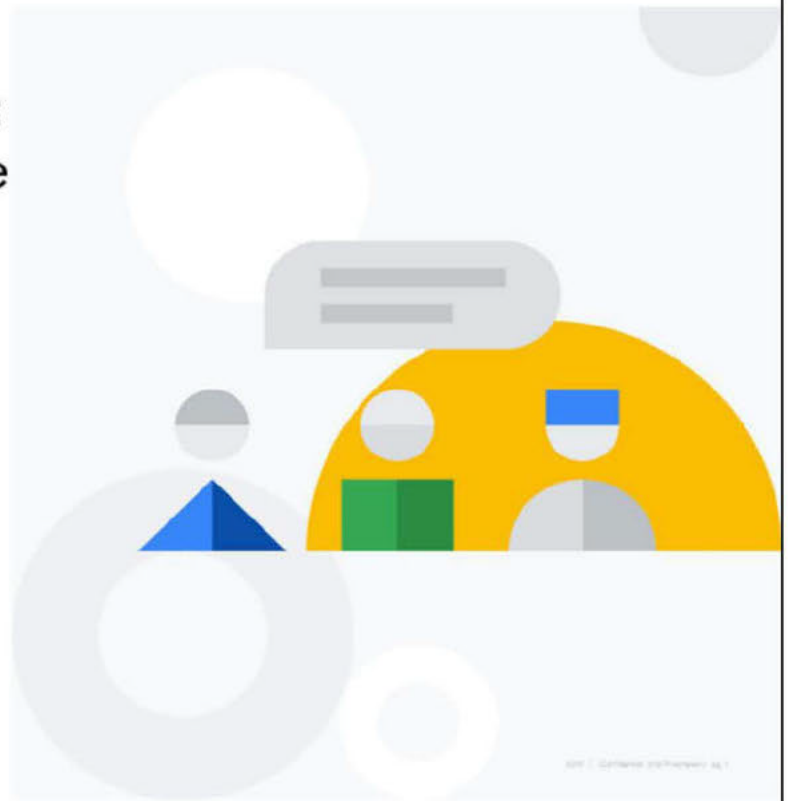
L.

EXHIBIT 6

Redacted Version of Document
Sought to be Sealed

KOF Research Review: Reputation Council Update

June 2021



© 2021 Google LLC. All Rights Reserved.

© 2021 Google LLC. All Rights Reserved.

Brand Studio
insightslab

Goals for today:

1. **Educate:** Systems in place to understand KOF sentiment/action
2. **Go Deep:** KOF IQ
3. **Discuss:** Gaps / asks

Why KOFs?

1. Significantly more pressure from KOFs globally
2. More marketing investment than ever before
3. Increased research demand; new systems in place

google_l
ogo

© 2022 Google LLC. Confidential and Proprietary. All Rights Reserved.  insightslab

What can we learn from KOF IQ?

EMEA

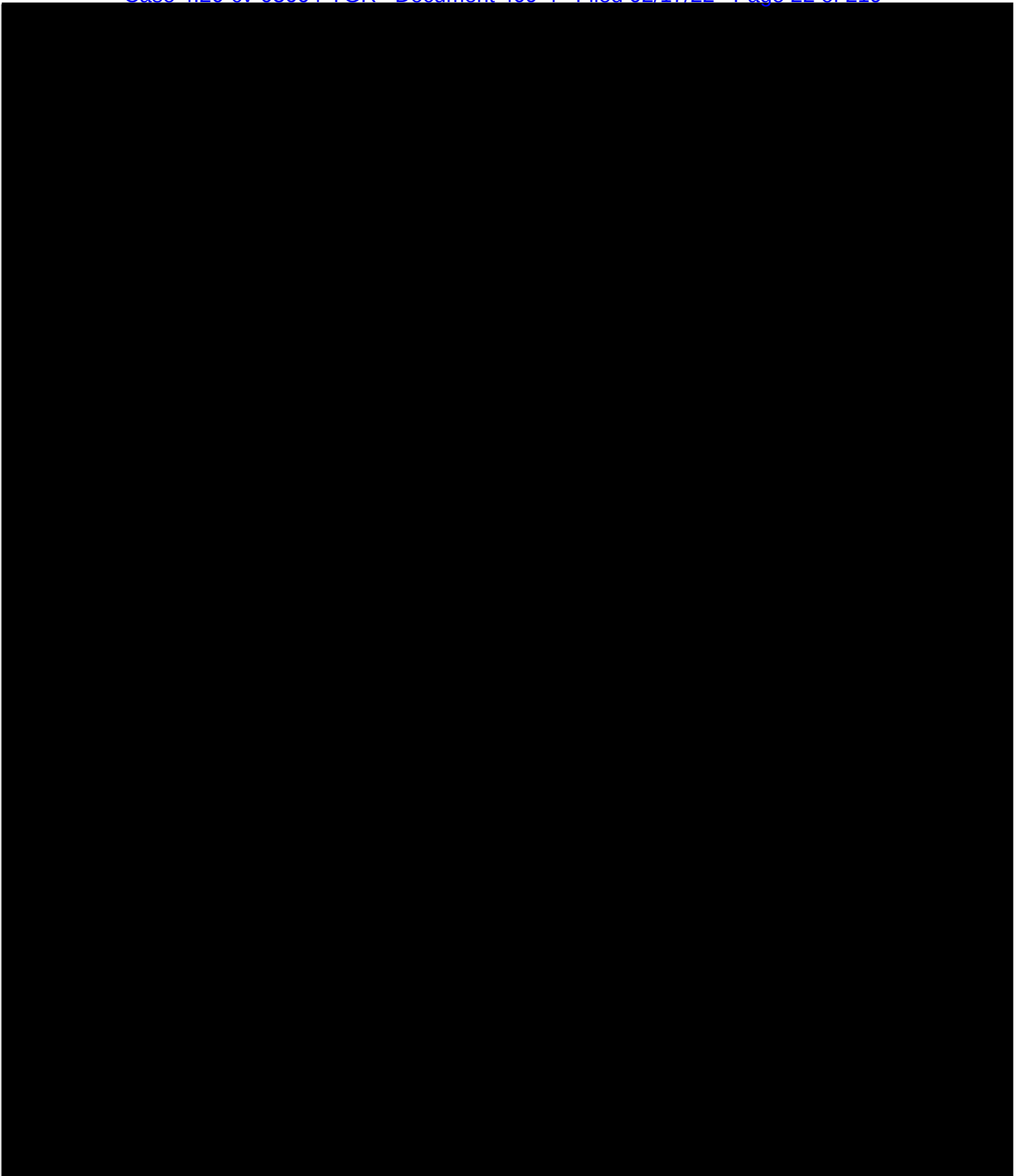
google_i
ogo

© 2022 Google LLC. Confidential and Proprietary. insights:lab

- KOF Social Listening has been running in EMEA for the past few years (since 2018 for KOF, and 2017 for consumer) but this year we transitioned to a globally aligned structure

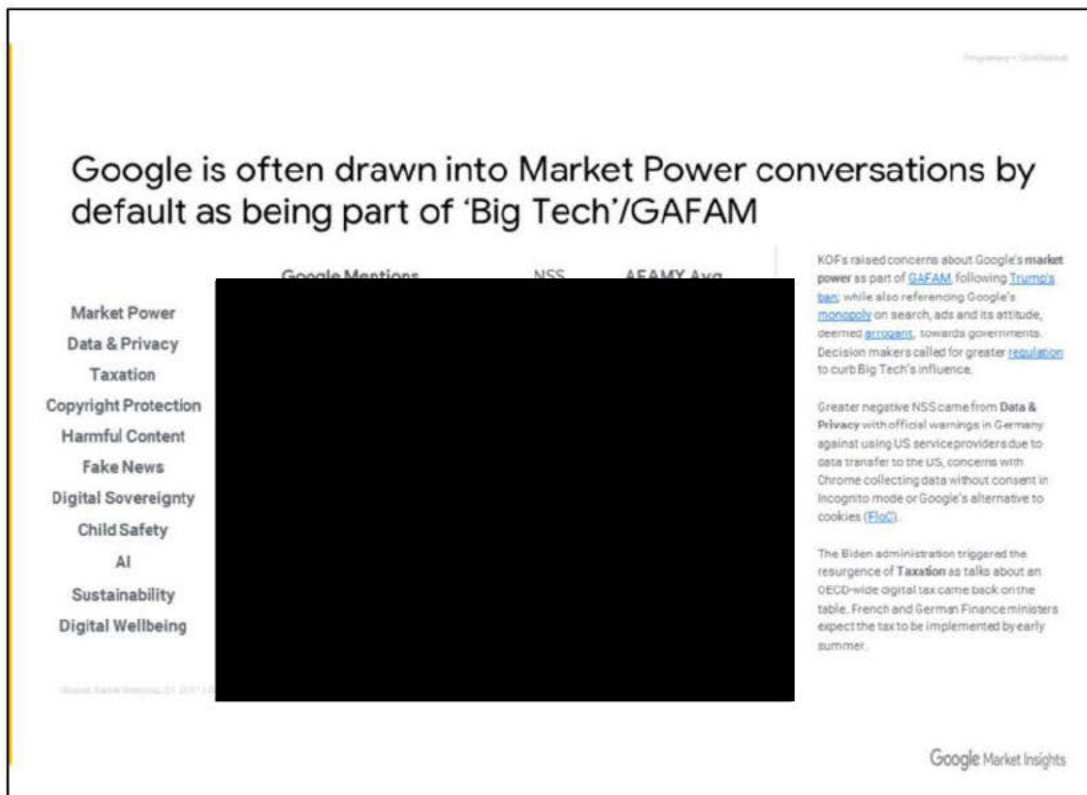
- [REDACTED]
- [REDACTED]

[REDACTED]





- A Google KOF mention is when one of our KOFs is mentioned alongside Google. This includes mentions that are ones to be further analyzed and fall within our topic structure and those that fall outside such as a mention saying “Google posted record sales”, or passing mentions of Google in a side headline.
- A KOF All Topic Google mentions are mentions that fall within Corporate Responsibility, Economic Contribution, Technology, Products, Initiatives & Events.
- KOF Main Topic Google mentions are those that fall within Corporate Responsibility, Economic Contribution or Technology.



- This is taken from our recently released qrtly report
- One key learning from is that Google is being grouped together with GAFAM as 'big tech' and this is impeding our overall perception
- Several years ago, we saw in Europe that Google and Facebook were consistently mentioned in tandem. Google took decisive steps to differentiate (in terms of Policy approach) ahead of the Cambridge Analytica scandal, and this lessened the damage
- This is something that we need to address again in Europe, as it exacerbates 'market power' perceptions and we actually see Google sentiment is more positive when discussed in isolation of other 'big tech'
- Data and tax are the other key issues in Europe



EXHIBIT 8

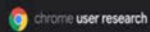
Redacted Version of Document
Sought to be Sealed



This deck has been presented as part of a virtual Chrome Incognito Roadmapping Workshop in March 2020. Participants: feuunk@rhalavati@, roagarwal@, rorymcclelland@, sabineb@, sideyilmaz@, yuanchen@ (moderator), lachner@ (moderator)

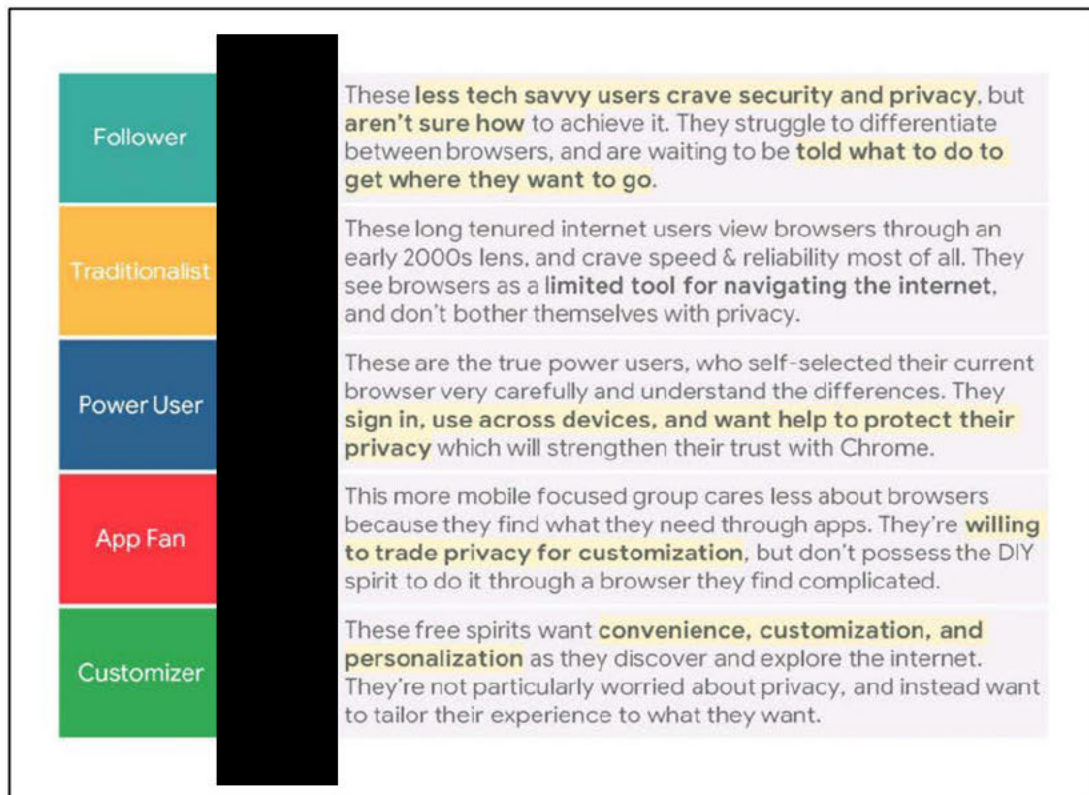
Click [here](#)

for the full workshop slide deck. Go on for the UXR lightning talk.



Confidential & Proprietary 2


Chrome User Segments (US)



The UX Research Archive has [redacted] “incognito entries”*

I did not study all :-) but skimmed quite some of them and compiled main meta-level insights.

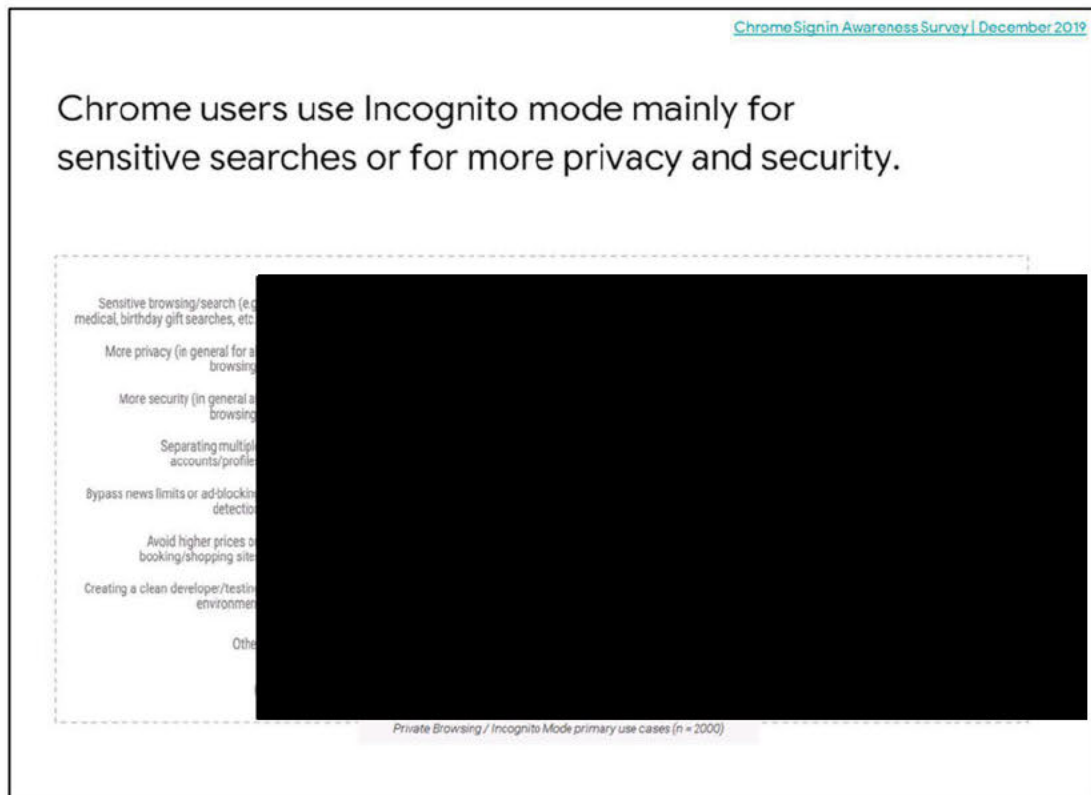
Let's go.

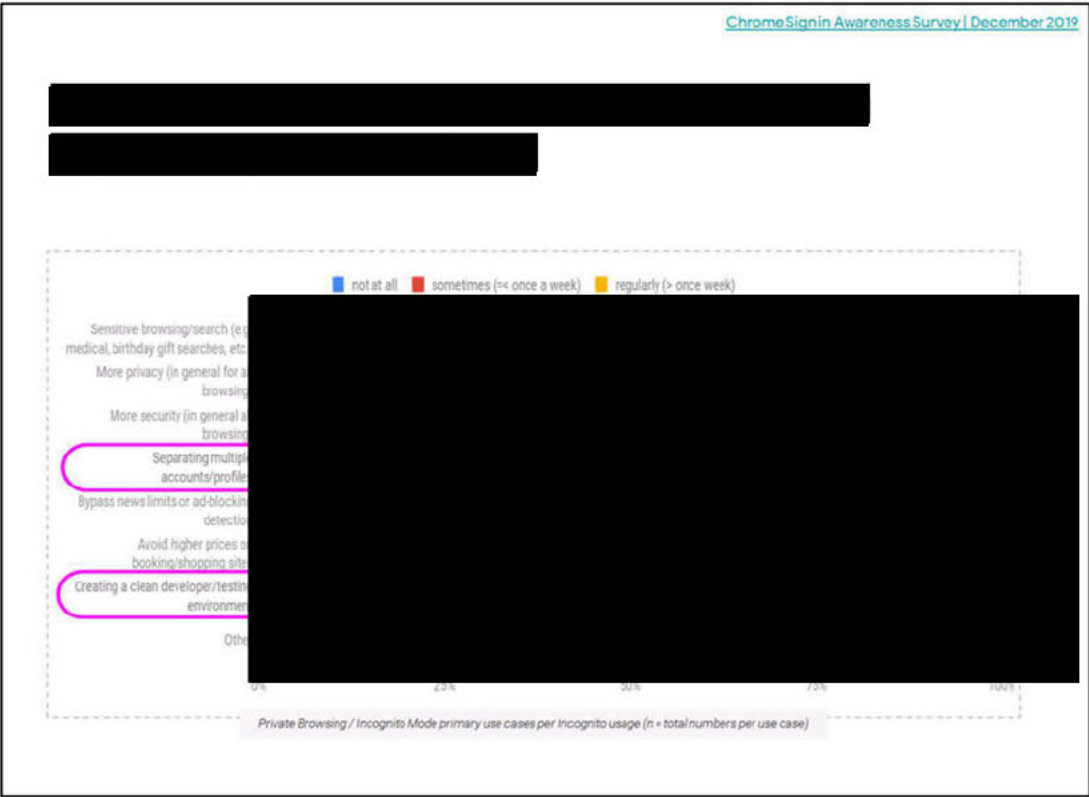


* as of 03/20/2020

- Chrome
- Chrome
- YouTube
- People & Identity
- Settings
- Privacy & Security
- Ads
- My Recent History
- Maps
- Way
- Location
- Account
- News
- Personalized
- Android
- Play
- Assistant
- Talkback
- Cloud Platform
- Sandboxing
- Hardware
- Cloud Platform
- Access
- Universal Design
- Remote

Use Cases







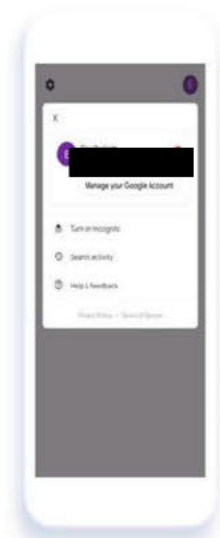


Identity-related vs. Context-dependent Use

OneGoogle | June 2019

Users see Incognito as a “Mode”.

When asking the participants if incognito is a mode, a state, a type of an account or something different, all participants describe that “incognito is a mode”.



Assistant | July 2019

Evidence differs with regards to personalization.

A Google Assistant version that still “knows them” seems very appealing

- Many users said that a version of “private mode” that they would use is one that doesn’t record any interactions, but may still use information about them.
- Users had a variety of opinions for what information it should remember about them from before the “private session.”
- Unclear how many would actually use this - but the existence itself is comforting.



Incognito Users*: What if Feature [X] is Implemented in a more Privacy Observant Manner? (N = 99)

* Uses Incognito at least once per month

Misconceptions & Expectations

What do users think private modes are? What does it do or not do?
Do users understand what works or doesn't work when they are in the mode?

- **Participants overestimate private mode protections.** There are several common misconceptions about private mode, including that it prevents all external parties from accessing user data and search history, safeguards against hacking, and protects against tracking and ad targeting... gives anonymity, obscures location, hides browsing activity from Google...
- **Participants do not understand how private mode works.** Although participants understand search history and cookies are not saved in private mode, they do not understand its technical mechanisms or that private mode has limited protection against external parties.
- **Participants expect limited functionality in private mode.** There is some evidence that participants don't expect websites/applications to fully function in private mode.



Tactical Research

Do users expect private modes to stay on for all future sessions until they turn it off? How would participants react to having their private session expire after a certain period of time? Indirect evidence...

- **expect to manually terminate private sessions.** Participants generally understand that they must exit their private browser to end their session.
- **like automatic timeouts of private sessions.** Some participants are concerned their information will be made vulnerable if they forget to end their session. Automatic timeouts may make them feel more secure, and participants already expect automatic session terminations when logged into sensitive accounts (i.e. banking, healthcare sites).
- **appreciate system reminders.** Some participants find it difficult to tell when they are in public vs. private mode. Given the concern about forgetting to end a private session, better indicators about the status of a private session may help participants feel more secure.

Geo UXR | March 2019

But, auto-expire is differently perceived.

Background:

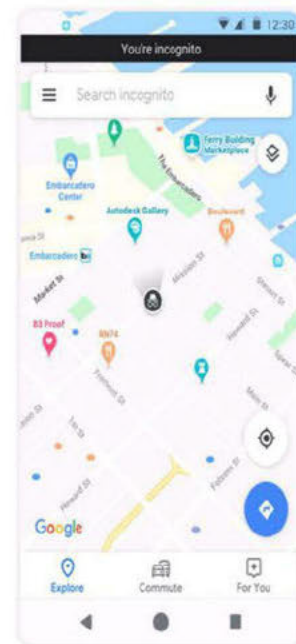
- + This study aims to understand users' motivations for and expectations of using Incognito mode in GMM.

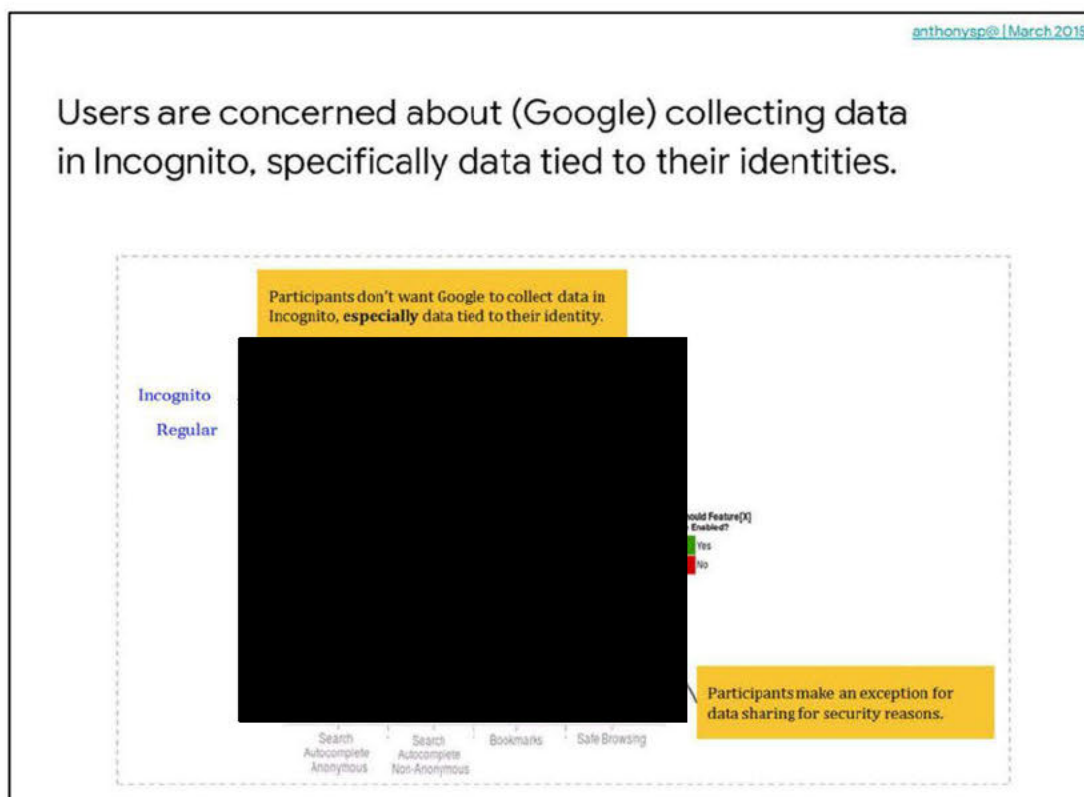
Auto-expire:

- + Auto expire did not resonate with users; almost all expected the session to remain on permanently.

Data storage:

- + Most ppts expected their location history to be private at the GMM account and device levels. There was no consensus on whether or not Google saved this information. Several expressed disappointment, but not surprise at the prospect of Google saving this data.





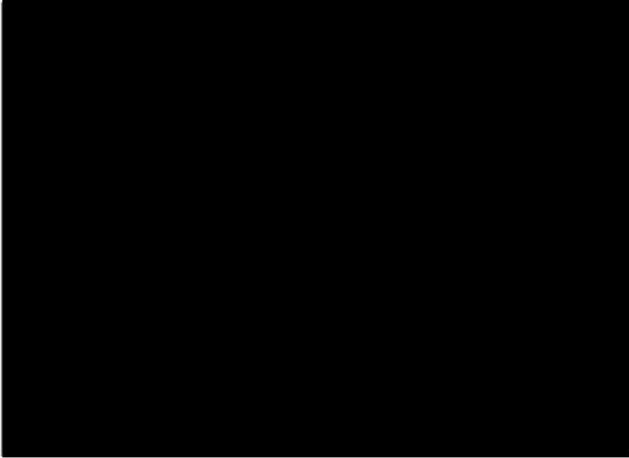

Incognito Users*: Should Feature [X] be enabled in Regular vs. Incognito (N = 138)
 * Uses Incognito at least once per month

What are any risks or potential moments when trust might be lost with participants while in private mode?
How can these risks be mitigated or minimized?

- **Not being made aware of private mode limitations.** Given that participants overestimate private mode protections, participants are surprised and feel misled when made aware of private mode vulnerabilities.
- **Being shown ambiguous or misleading disclosures.** Although participants often click through or ignore disclosures, disclosures should be difficult to ignore in order to clear up misconceptions and mitigate potential trust violations.
- **Having personal information leaked.** Settings that clearly show when they are in private mode, easy control of the mode, and control over information sharing may mitigate this concern.
- **Receiving targeted ads or suggestions.** Unless it is clearly disclosed that their activity may be trackable, receiving targeted ads or suggestions based on private mode activity may erode trust.

Chrome Study | January 2019

But, in-context user education is challenging due to brevity of strings.

- "Your identity will be visible to this site when you sign in."
- "Signing in will reveal your identity to this site."
- "Signing in will reveal your account and activity to this site."
- "Sites will be able to see your account and activity when you sign in."

No statistically significant differences between any group ($p = \text{[REDACTED]}$).

Branding, Awareness

Chrome UXR | August 2015

What does the term Incognito communicate?



What does the term Private Browsing communicate?



Not necessarily bad but simply different.
Incognito mode has an established
branding (in established markets).

[Brand Tracker US | November 2019](#)
[Brand Tracker IN | January 2020](#)



of respondents are
aware of incognito
mode (11/12)
(among those aware of Chrome)



of respondents are
aware of incognito
mode (07/20)
(among those aware of Chrome)

NBU

Sharing, security, and gender shape privacy in NBU.

Consider privacy strategies

- [REDACTED]
- [REDACTED]

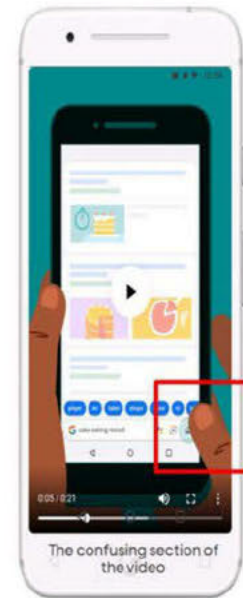
But

"I don't know. Based on the icon, it could be an app for **information about cars**. But I have no idea as to why it is given here."



NBU users are not familiar with Incognito Mode.

- Some words in the disclaimer text (particularly “school”, “employer”, and “internet service provider”) confuse participants.
- A Mini Learning video aided comprehension, and most said they understood the main purpose of Incognito after watching. However, only a few could demonstrate its use.
- Most understood the **No History** concept from the Mini Learning Video



UXR Recap

You've gone Incognito. Have you?

[REDACTED]

T [REDACTED]
[REDACTED]

[REDACTED]

T [REDACTED]
[REDACTED]

[REDACTED]

T [REDACTED]
[REDACTED]

[REDACTED]

T [REDACTED]
[REDACTED]

[REDACTED]

T [REDACTED]
[REDACTED]
[REDACTED]

EXHIBIT 9

Redacted Version of Document
Sought to be Sealed

The Incognito Problem

Chris Palmer (palmer@)

Key Fact:
Incognito
Confuses People

"Incognito" Confuses People

We know from intuition, anecdotes, and now empirically ([Yuxi Wu, et al.](#); see also [Habib, et al.](#)) that the "incognito"/Spy Guy branding, and the complex disclosures (like all complex disclosures), confuse people as to what exact guarantees it offers and does not offer.

Ironically, across all browsers, Chrome's disclosures were the least confusing by a modest amount. But it's still bad.

Id	Date	Text
1	07/22/2018 07:53:36	It'd be good to try to replicate or further validate the study, but I'd be surprised if we got a significantly different result.

WWW 2018, April 23–27, 2018, Lyon, France

Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar[†], Sascha Fahl[‡], Blase Ur

Table 5: Scenarios where participants held misconceptions, shown with the correct answers and percentage of participants who gave incorrect answers. For comparative scenarios, (in)equality symbols denote the correct answer, and we give the sum of all participants answering otherwise.

Scenario	Answer		% Incorrect	
	Std.	Priv.	Std.	Priv.
<i>Overestimating private mode's privacy protections</i>				
Search queries associated (logged in)	Yes	Yes	1.5	56.3
Bookmarks saved across sessions	Yes	Yes	25.4	46.5
Geolocation can be estimated	Yes	Yes	5.2	40.2
Employer can track browsing	Yes	Yes	1.1	37.0
Better protected from viruses/malware	Std. = Priv.		27.1	
IP address can be collected	Yes	Yes	0.7	25.2
Government can track browsing	Yes	Yes	4.1	22.6
ISP can track browsing	Yes	Yes	3.0	22.0
<i>Underestimating private mode's privacy protections</i>				
Downloaded file in browser's list	Yes	No ^a	1.3	51.7
Proportion of targeted ads	Std. > Priv.		30.9	
Search queries associated (not logged in)	Yes	No	20.2	30.0

^aExcept in Brave's private mode, which does retain download history

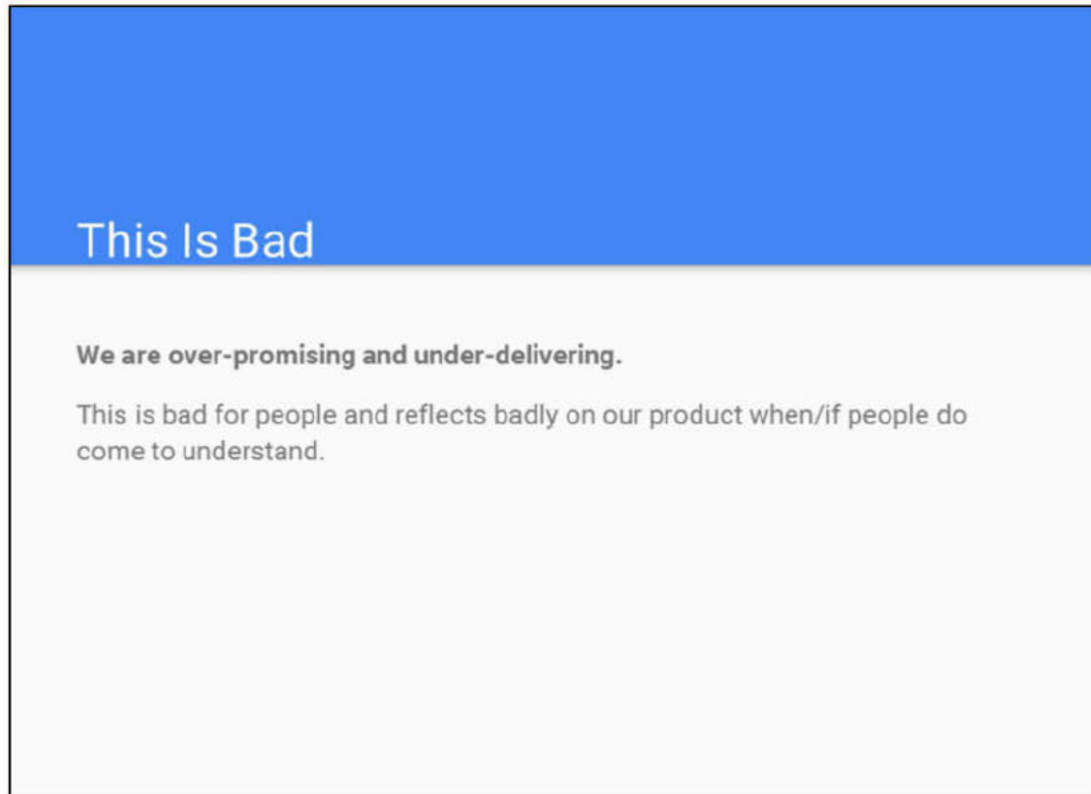
Table 6: Distinguishing scenarios where private mode's impact depends on the browser or context.

Scenario	% Yes	
	Std.	Priv.
Items in shopping cart saved across sessions	97.8	78.8
Browser extensions active across sessions	98.3	69.1
Forensic expert can reconstruct browsing history	98.7	52.8
Site-specific preferences (e.g., for pop-ups) saved	98.3	31.3

Table 7: Distribution of responses for comparative scenarios where the impact depends on the browser or context.

Scenario	% Responses		
	Std. > Priv.	Std. = Priv.	Std. < Priv.
Amount of ads	32.2	64.9	2.9
Page loading speed	24.8	53.6	21.6

($\chi^2(12) = 38.1, p = .001$). In the control condition, 32.4% of participants mistakenly believed downloaded files would still be listed in the browser. A higher proportion of participants in Brave (62.2%,



This Is Bad

We are over-promising and under-delivering.

This is bad for people and reflects badly on our product when/if people do come to understand.

Key Question:
What Do People
Use Incognito
For?

Why Do People Use Private Modes?

From Wu, et al.:

1. Hide browsing history, especially visits to adult websites;
2. prevent targeted ads and search suggestions;
3. achieve "safer" browsing;
4. Prevent browsers from saving login-related information;
5. avoid cookies;
6. accommodate intentional or unintentional use by others.

Id	Date	Text
1	07/23/2018 13:28:04	what's the motivation here? how does this differ from 2?
2	07/23/2018 13:28:04	This is a list of reasons that people reported to the researchers for why they use private browsing modes. Part of the point of the research is that people don't fully understand the mechanisms.

Incognito Is Overloaded

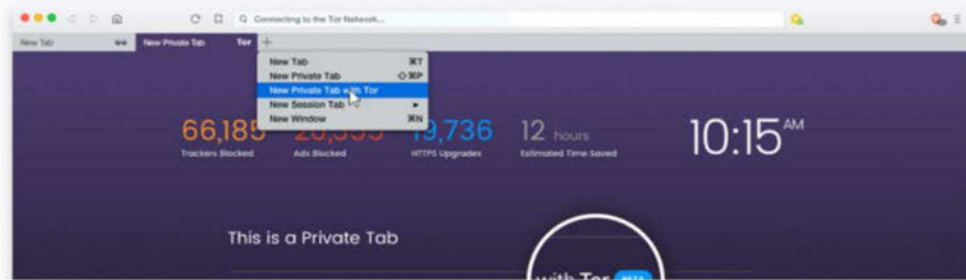
Those 6 reasons are related but different. Perhaps we really need multiple modes (we've already got Guest mode)?

Or more and easier affordances for privacy and control in Settings/elsewhere?

Key Fact: There's
A Privacy Feature
Race

Brave Introduces Beta of Private Tabs with Tor for Enhanced Privacy while Browsing

by Brave | Jun 28, 2018 | Announcements, Features, Privacy



A Firefox Competitive Advantage

The Tor Project developers said that Project Fusion has the accord of Mozilla's CEO and CTO, which probably means it has a high chance of coming to fruition. However, many issues have to be considered first, such as developing private telemetry, fixing the problem with fingerprinting resistance breaking websites, and so on.

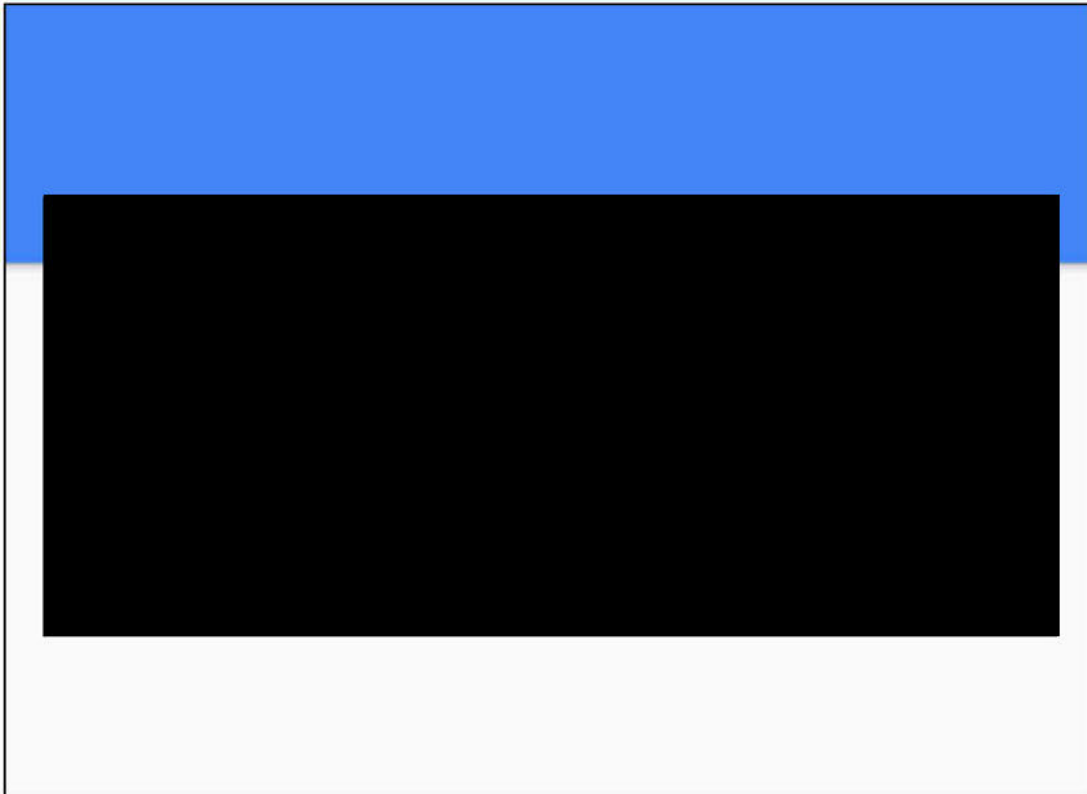
Additionally, Mozilla wants to first standardize the Tor client specification, write conformance tests for it, and open the documentation. All of that means that more people could look at how Tor is implemented in Firefox and see if there are any issues with that implementation.

The main reason why Mozilla would even want to integrate Tor into Firefox is because it could provide its users real private browsing, something that most competitors will not be able to offer. Mozilla has taken an increasingly strong pro-privacy stance in the past few years, and Project Fusion could further boost its pro-privacy image.

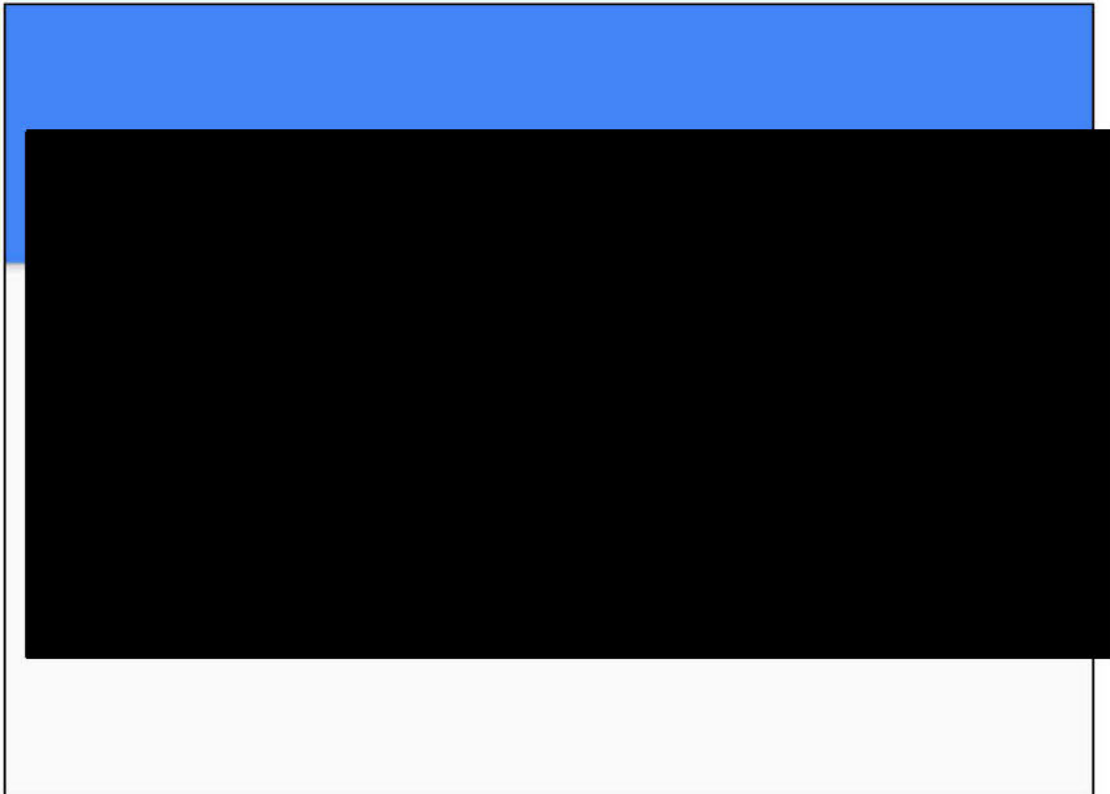
It could also put Firefox in a much more direct contrast with Chrome, a browser developed by Google, which is heavily invested in user tracking in order to serve more targeted ads.

ITP, ITP2, ITP3

Safari and Mozilla are moving in this area, and we'll need to have some kind of response as well.

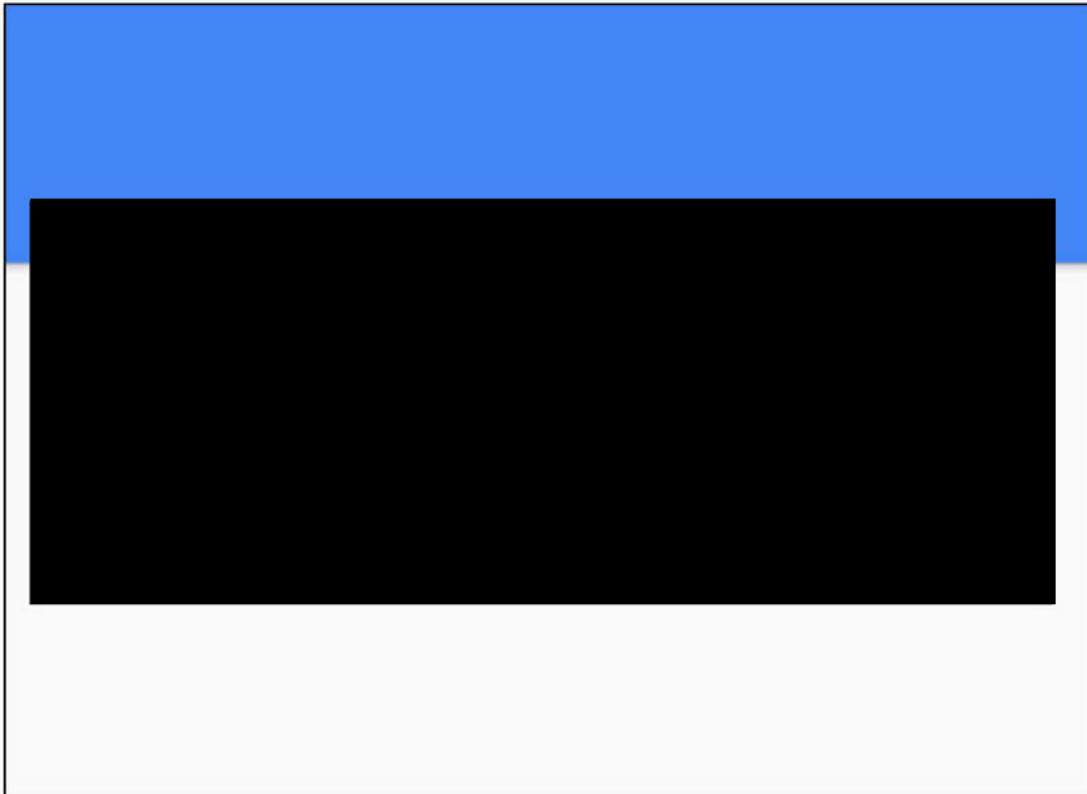


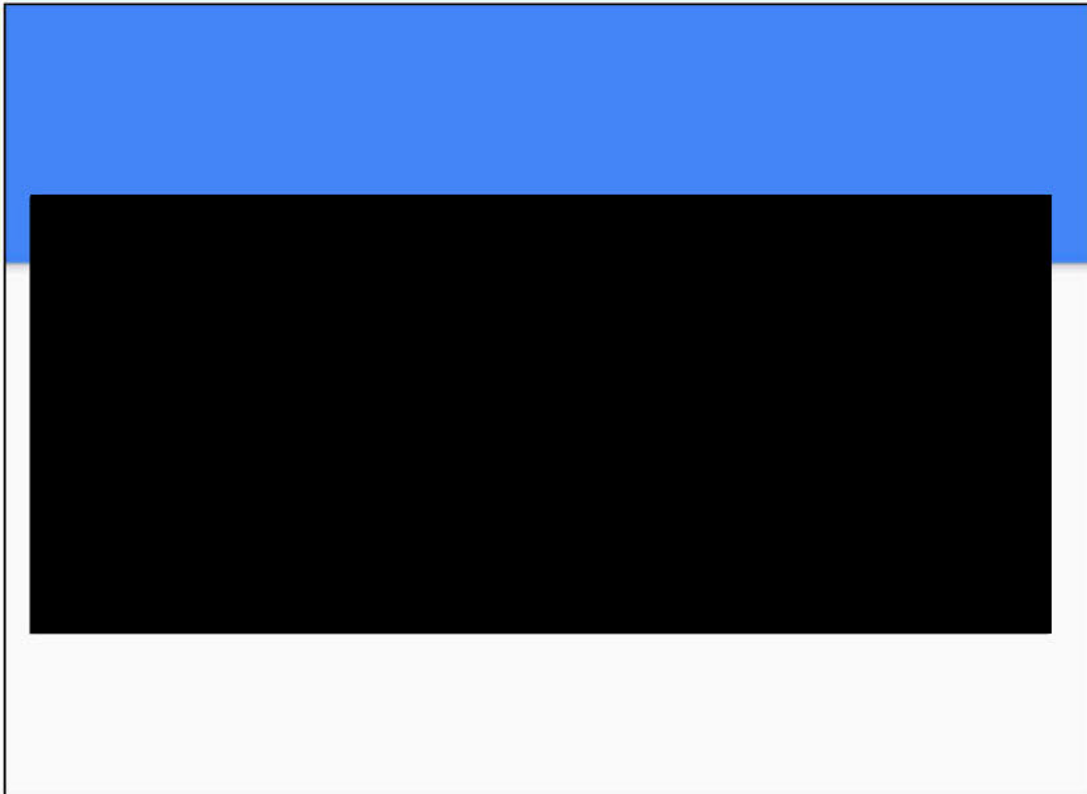
Id	Date	Text
1	07/21/2018 14:10:10	



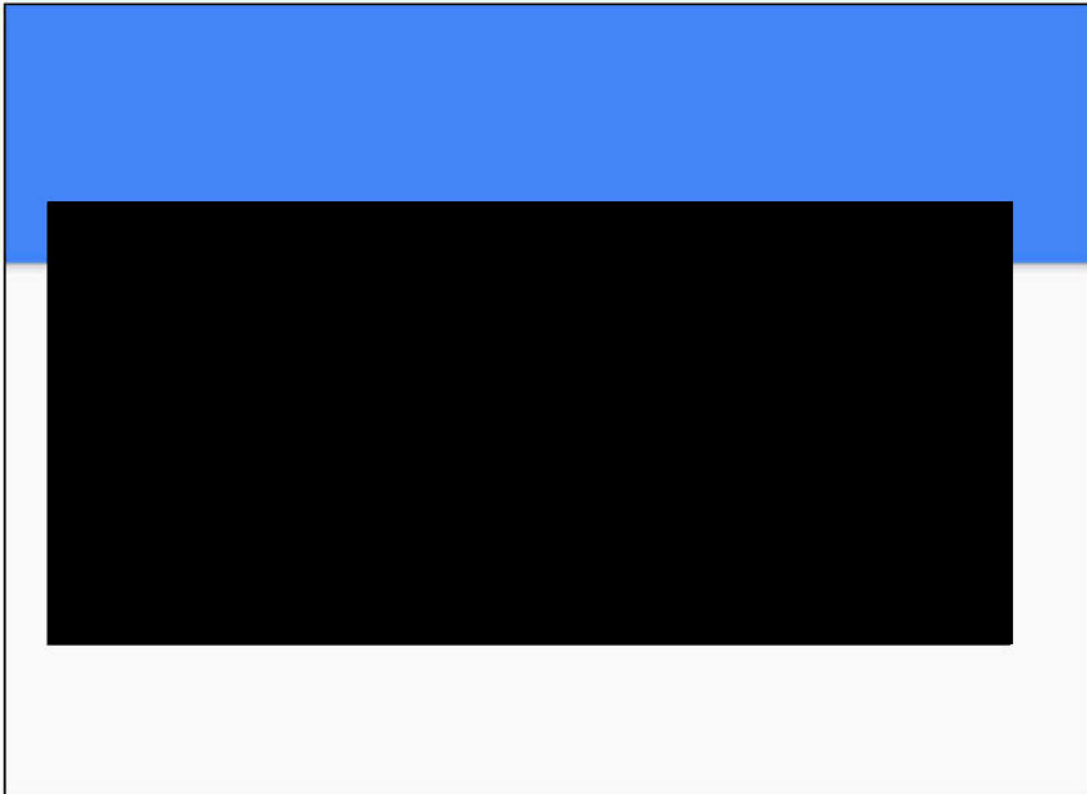


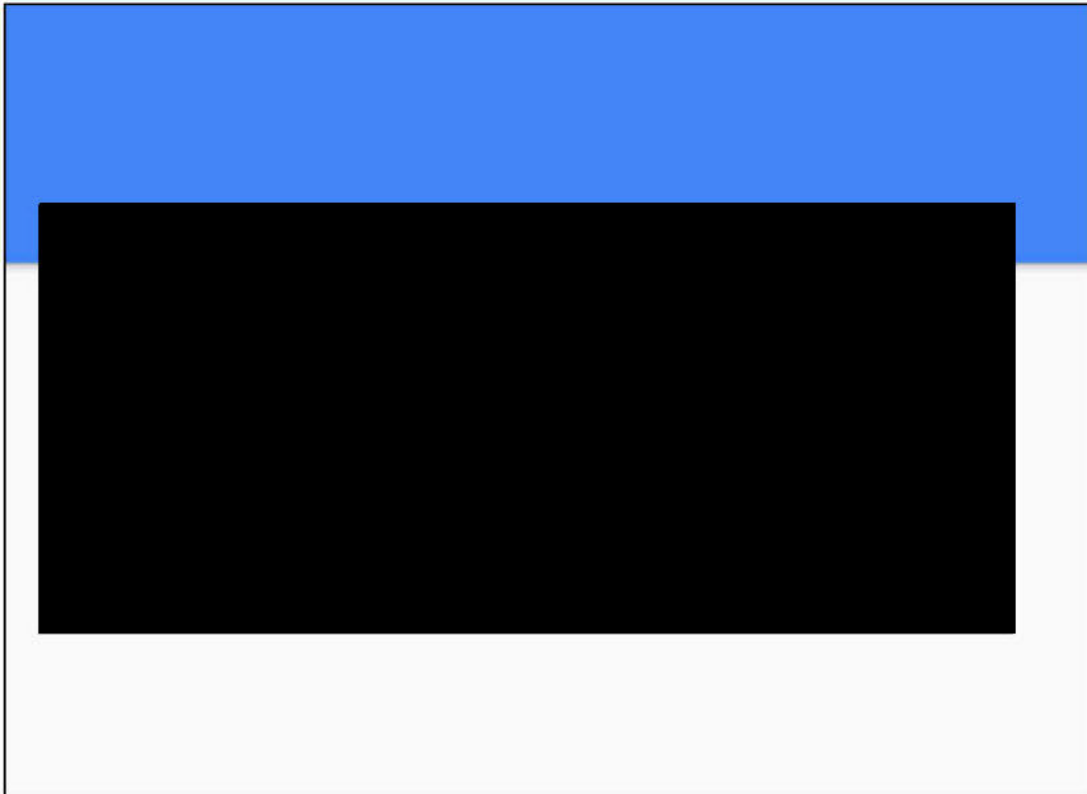
Options

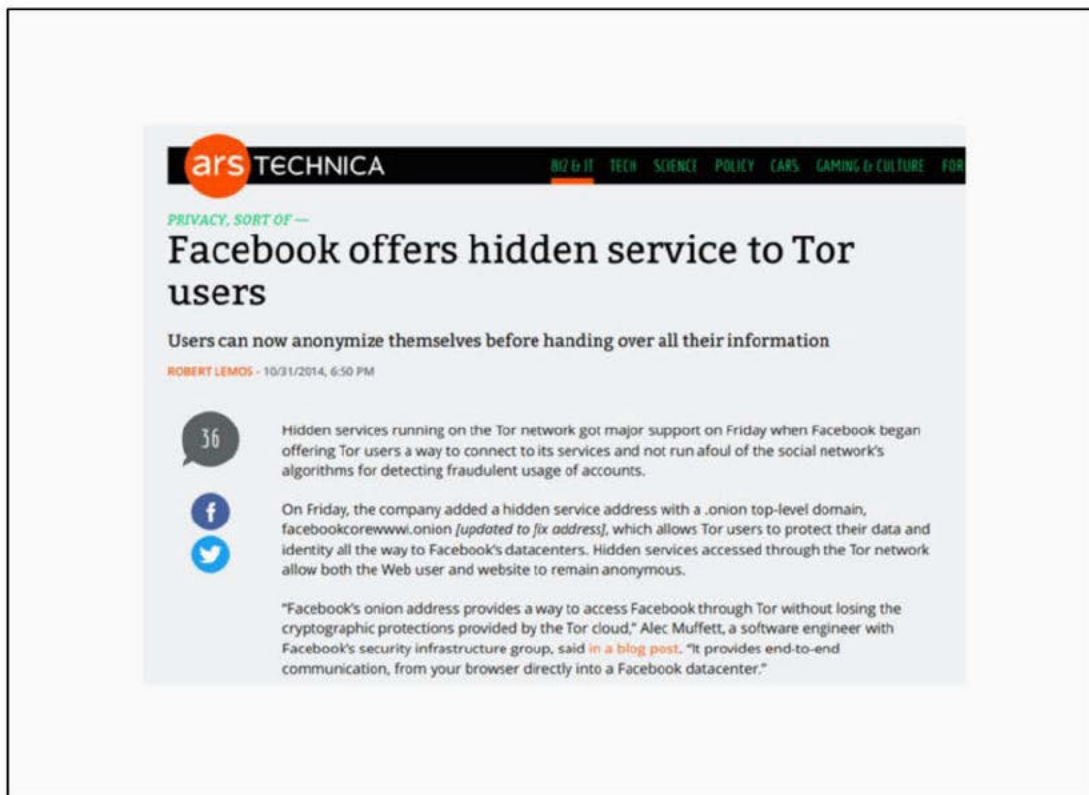


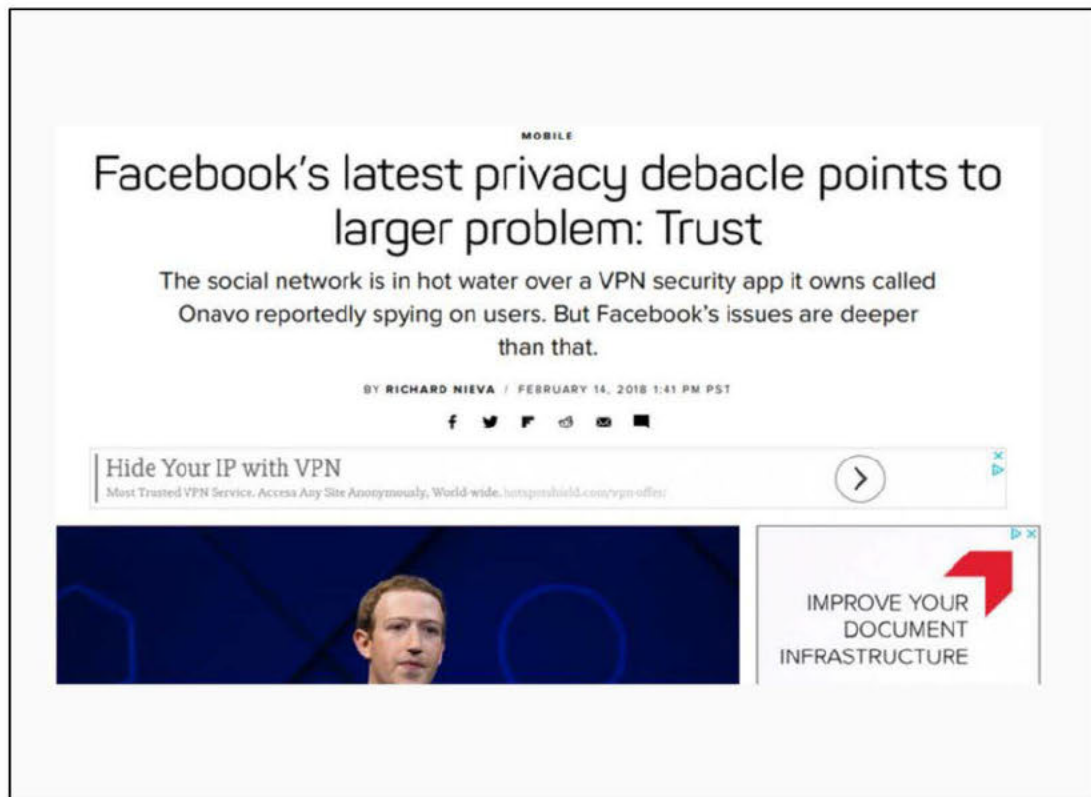


Id	Date	Text
1	07/23/2018 14:04:19	[REDACTED]
1	07/23/2018 14:05:29	[REDACTED]
2	07/23/2018 14:05:29	[REDACTED]









Most VPN Services are Terrible

Short version: I strongly *do not* recommend using any of these providers. You are, of course, free to use whatever you like. My TL;DR advice: Roll your own and use [Algo](#) or [Streisand](#). For messaging & voice, use [Signal](#). For increased anonymity, use [Tor](#) for desktop (though recognize that doing so may actually [put you at greater risk](#)), and [Onion Browser](#) for mobile.

This mini-rant came on the heels of an interesting twitter discussion:
<https://twitter.com/kennwhite/status/591074055018582016>

Again I strongly *do not* recommend using any of these providers.

Provider / known "Secret" Key

```
Astril / way2stars
EarthVPN / earthvpn
GFWVPN / gfwvpn
GoldenFrog / thisisourkey
IBVPN / ibVPNsharedPSK!
IPVanish / ipvanish
NordVPN / nordvpn
PrivateInternetAccess (PIA) / mysafety
PureVPN / 12345678
SlickVPN / gogoVPN
TorGuard / torguard
TigerVPN / tigerVPN
```

source: <https://gist.github.com/kennwhite/1f3bc4d889b02b35d8aa>

There Is Some Opportunity, Though

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

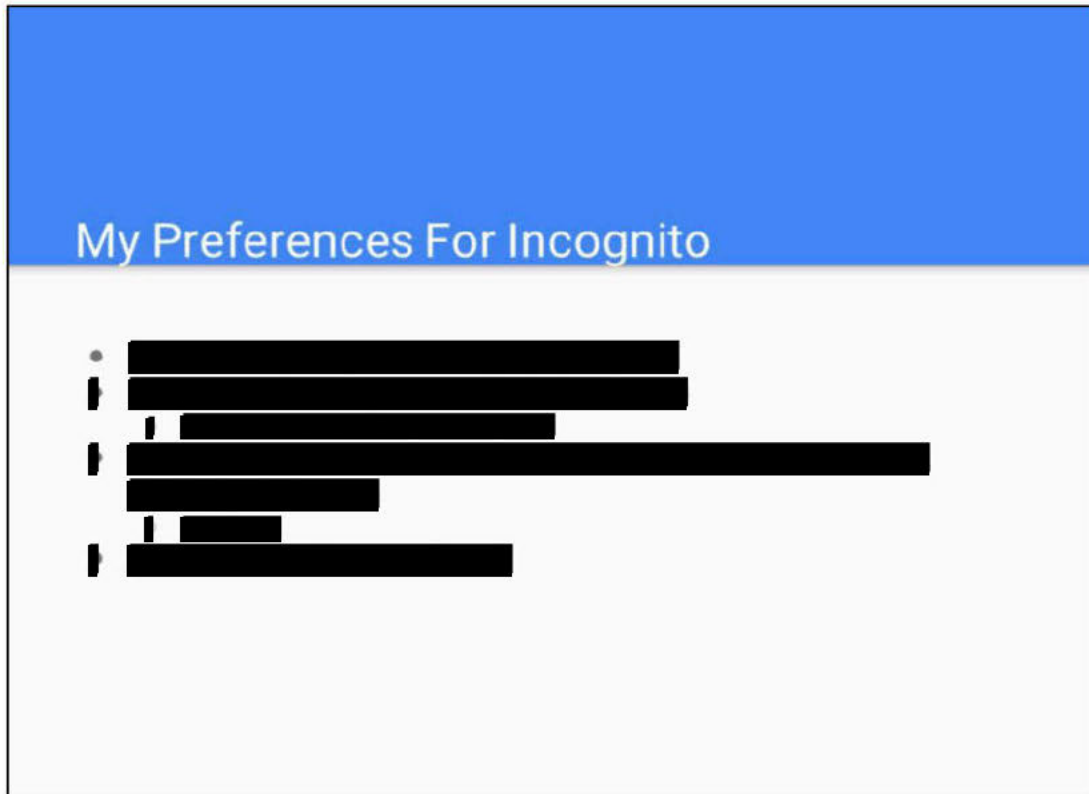
[REDACTED]

Key Question:
How Much
Breakage Will
People Tolerate?

Hypothesis: Not Much

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Conclusion:
Options, But No
Single Clear Path



Id	Date	Text
1	07/21/2018 15:50:53	[REDACTED]
3	07/22/2018 08:00:43	[REDACTED]
2	07/23/2018 12:54:42	[REDACTED]
3	07/23/2018 12:54:42	[REDACTED]

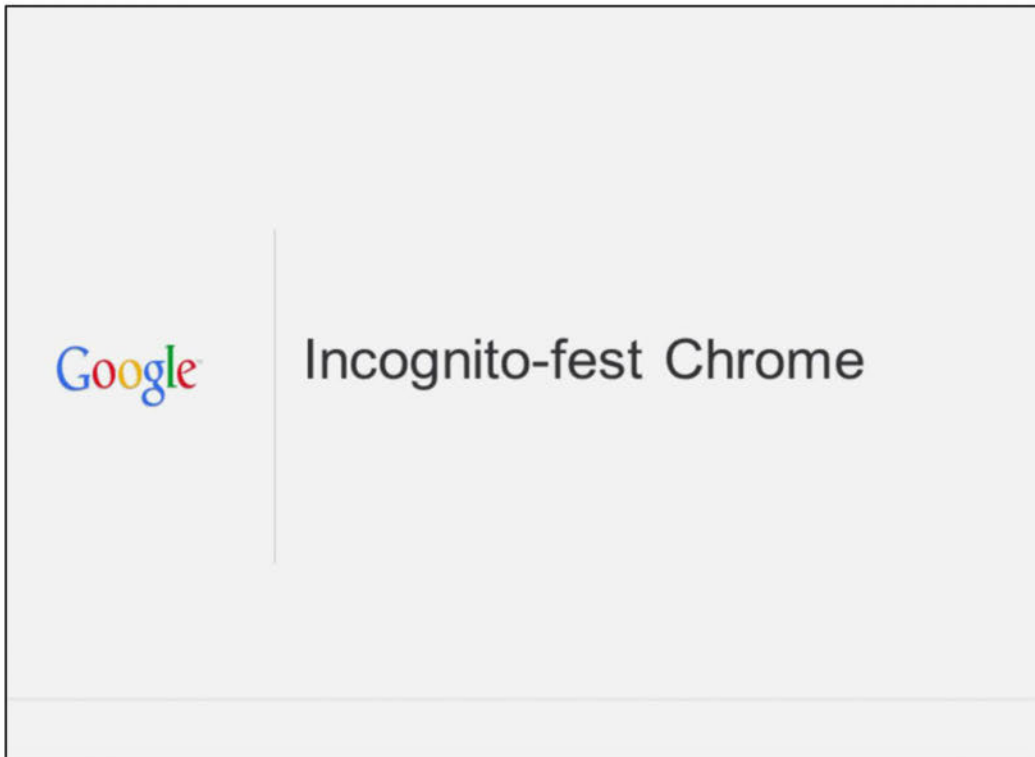
Additional Useful Efforts

- [REDACTED]
- [REDACTED]

EXHIBIT 10
Redacted in its
Entirety

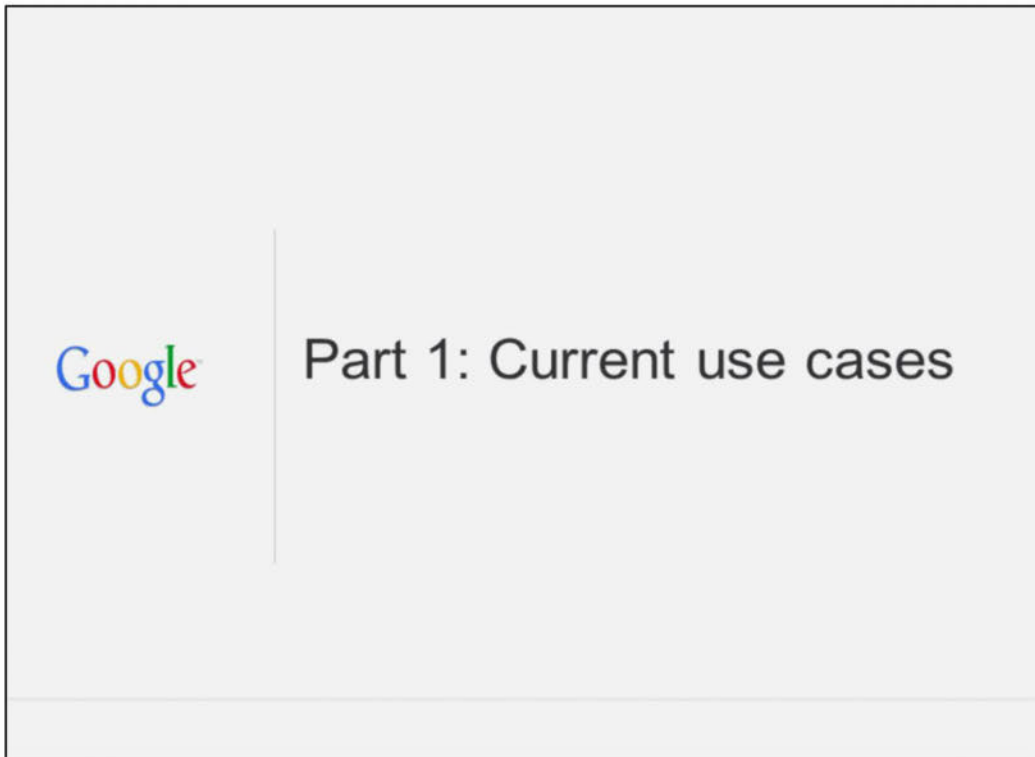
EXHIBIT 12

Redacted Version of Document
Sought to be Sealed





1. Current use cases
2. Current implementation
3. Challenges
4. Proposal







Currently supported use cases

- user wants to hide browsing activity to someone with access to the device (e.g. spouse)
- user doesn't want information about their browsing be tracked longtime on the internet (readvertising, records in search history)
- user doesn't want information about their browsing to be shared with Google

Google Confidential and Proprietary

Id	Date	Text
1	 02/25/2015 19:27:01	+battre@google.com Dominic, could you please review and add missing use cases, if any?

Google Confidential and Proprietary




Current promises

You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept. [Learn more about incognito browsing](#)

Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

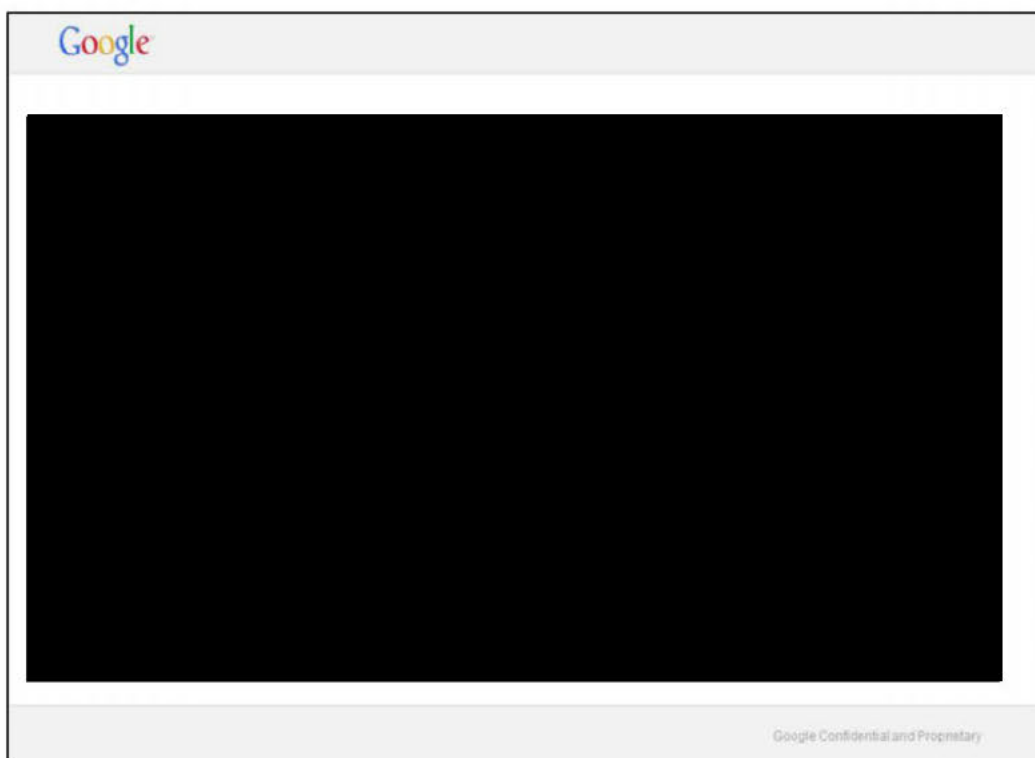


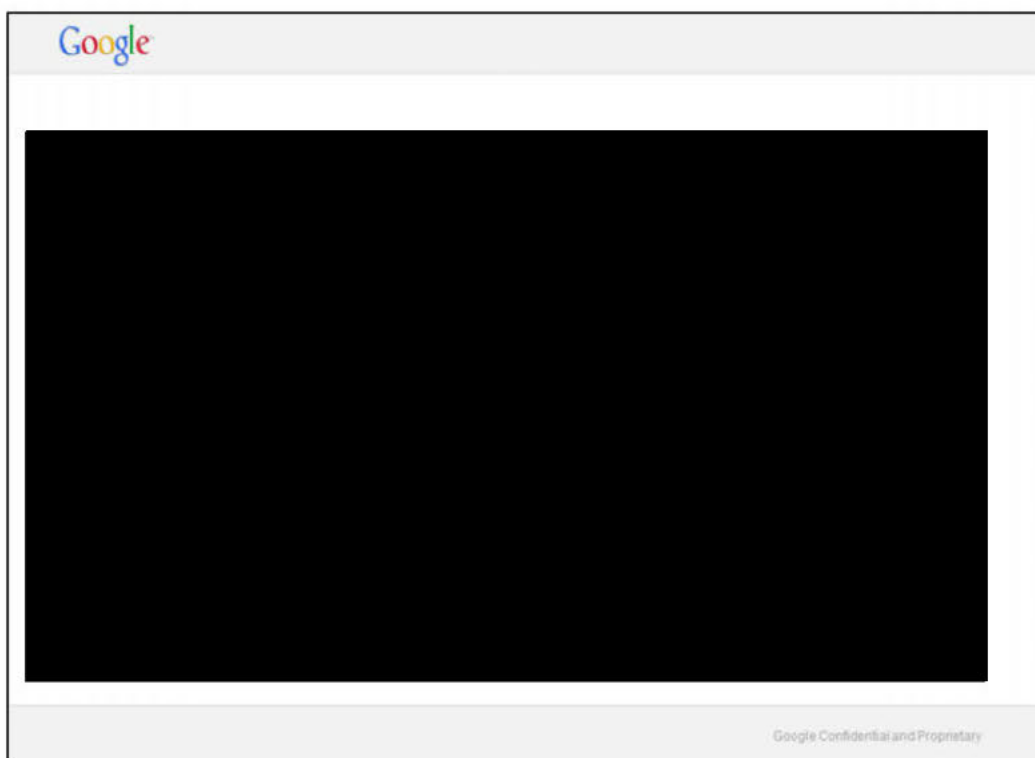
- The name "Incognito mode" might create the false expectation that you're invisible on the web
- [Help Center article](#)

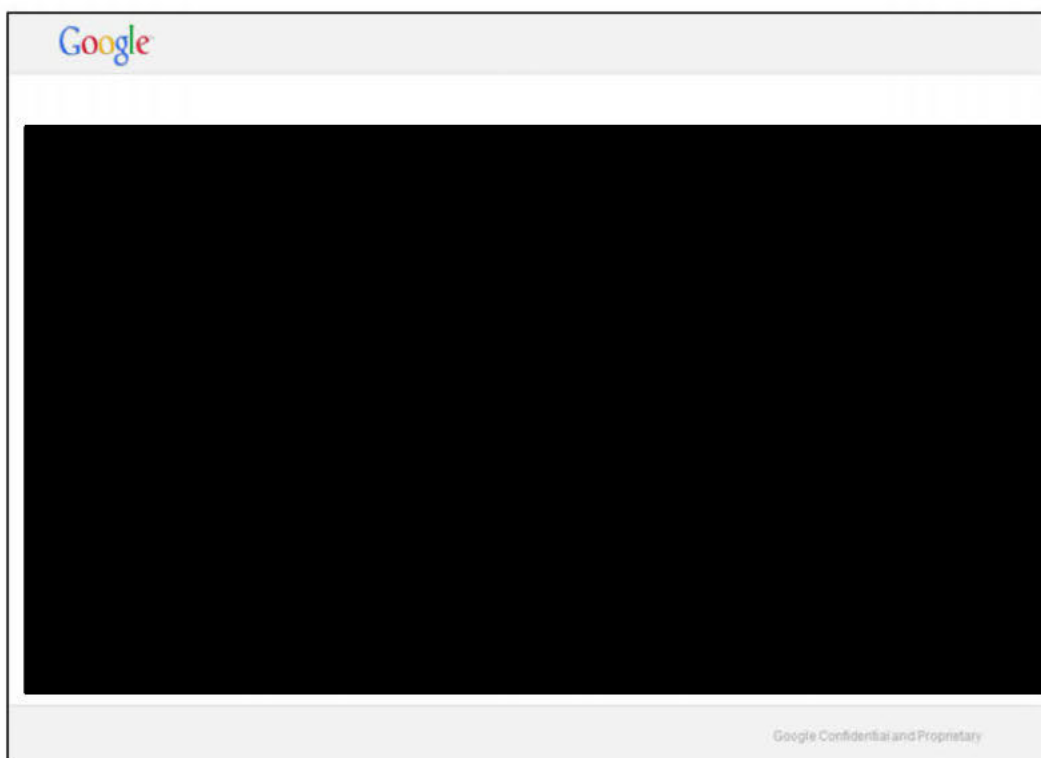
Google Confidential and Proprietary



Part 2: Current implementation









What else is incognito mode?

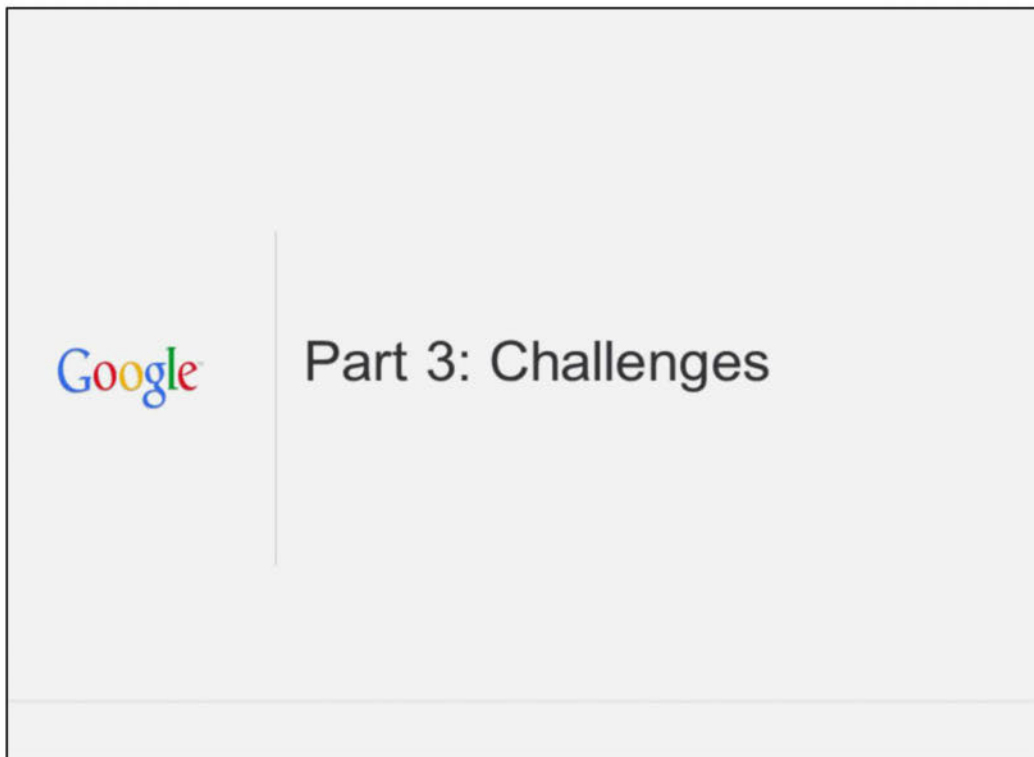
Don't talk to Google in the background

- Online spell-checking disabled
- URL auto completion disabled
- No geolocation in omnibar searches

Start with a fresh profile

- Empty local storage
- Passwords are only filled on user request

Google Confidential and Proprietary

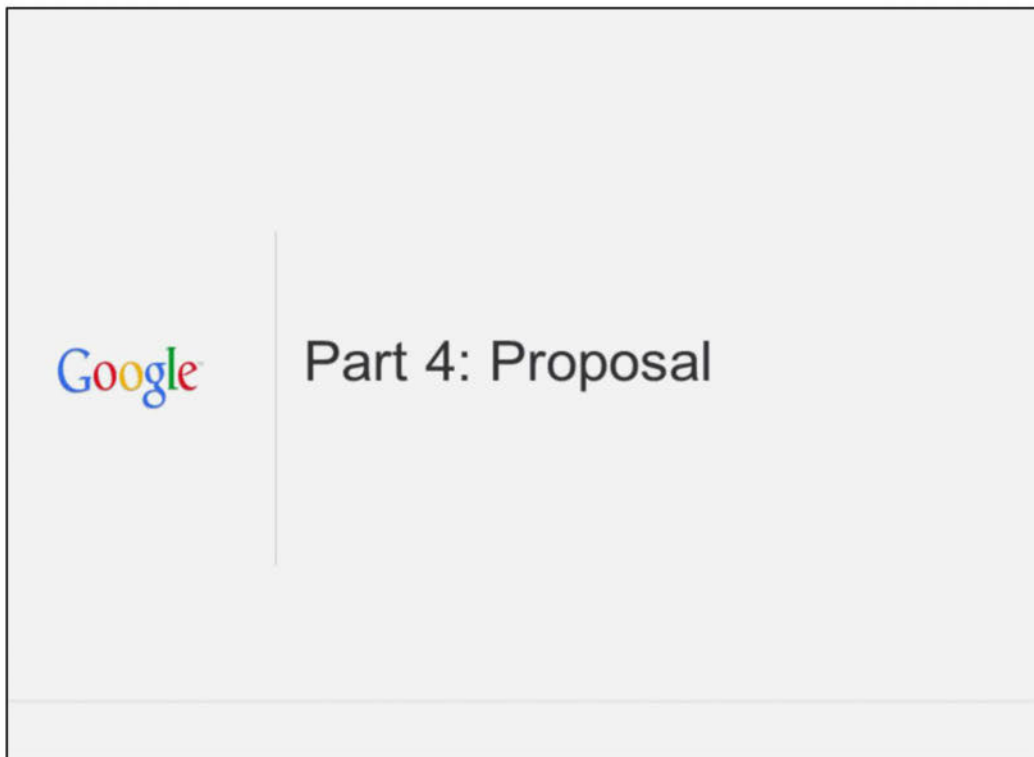




Challenges & limitations

- Misinterpretation of definition (see Eric Schmidt quotes)
- Tension about definition across teams (e.g. discussion on linkability due to HSTS)
- Limitations on iOS
- Finger printing

Google Confidential and Proprietary






Objective

- Keep it useful
- Keep it at least on a par with other browsers
- No degradation
- Decrease misunderstanding
- Allow users to trust Chrome when they don't want it to connect to Google

Google Confidential and Proprietary



Proposed definition

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Google Confidential and Proprietary

Id	Date	Text
1	02/26/2015 00:58:36	Deltas might help illustrate what the options are.
2	02/26/2015 14:42:29	<div data-bbox="545 220 1256 288" style="background-color: black; height: 33px; width: 462px;"></div> <div data-bbox="545 292 1264 333" style="background-color: black; height: 20px; width: 467px;"></div> <div data-bbox="545 333 1264 353" style="background-color: black; height: 10px; width: 467px;"></div> <div data-bbox="545 353 1001 435" style="background-color: black; height: 40px; width: 296px;"></div>
1	02/26/2015 14:42:29	<div data-bbox="545 445 944 466" style="background-color: black; height: 10px; width: 259px;"></div> <div data-bbox="545 486 1276 588"> <p>Sabine, I have added your proposal to the next slide.</p> <p>Garth, what you describe is something I explicitly do not want for two reasons:</p> <p>1) It puts us into significantly worse position when compared to other browsers in the press.</p> <p>2) I believe that we don't do our users a service. We have a solution that works for 99% of cases of the proposed definition. Ignoring 3rd party tracking leads incognito mode ad absurdum in my opinion.</p> </div>

Google Confidential and Proprietary





Unwanted events to be prohibited

- **People** walk up to computer and can see what user has done in incognito mode before.
- **Data leakage:** User is greeted in incognito mode with ads / account name / ... that transcended from a previous incognito session or regular mode.
 - We will add a disclaimer that explains the limitations (tracking by governments, employers, ...; tracking via fingerprinting).
- Users are surprised that **Google** gets information about their browsing while in incognito mode.

Google Confidential and Proprietary

Id	Date	Text
2	02/26/2015 14:43:20	Is this bad? There is some personalization currently in Incognito already. Having an account name is similar and would make sense if the branding matched it. (i.e. the mode was about forgetting activity during the session and not about being a spy)
2	02/26/2015 14:43:20	Which part are you referring to with your question whether this is bad?

Google Confidential and Proprietary





Fingerprinting

- Most users do not feel threatened by fingerprinting as long as it has no perceptible impact on their browsing.
- Major websites use it only for “good” purposes.
- Our position:
 - We condemn the use and make it harder (e.g. introducing noise into canvas fingerprinting)
 - We don't limit incognito mode functionality because somebody could use fingerprinting (if we accepted fingerprinting in the threat model, we would end up with a useless or non-existing incognito mode).

Google Confidential and Proprietary

EXHIBIT 13

Redacted Version of Document
Sought to be Sealed



Incognito-fest Intro

2.26.2015

<http://go/google-incognito>

CONFIDENTIAL



Goals for Today

1. Understand the history and current state of Incognito across Google.
2. Agree on goals of Incognito (supported use cases).
3. Understand product options. Define limited set of these.
4. Reach recommendation on the best option for the next version of Incognito across Google platforms.

Not Goals?

1. Find an actual brand?

Agenda

- Intro (this!)
- Chrome
- Android
- Internet of Things
- UER summary
- (break)
- Deep dive

Known: Incognito is successful

- Somewhere between [REDACTED] weekly actives in Chrome.
- Meets real user needs.

Implications

- Incognito is worth pursuing.

Known: The Brand is Wrong

- Users often misunderstand what Incognito does.
- “Incognito” implies spy-related functionality that we don’t want to provide.

Implications

- “Incognito” should be considered a placeholder name.
- We should decide on the best feature to build, then find branding that makes sense.



Known: We are in a cross-platform world

- Users move freely between platforms (Chrome, Android, iOS)
- Users have privacy needs on all these platforms.

Implications

- Incognito on multiple platforms makes sense.
- We need a consistent experience to aid in platform mobility.

Known: Guest, Incognito both make sense

- Guest provides a blank slate that enables sharing a device with a friend.
- Incognito is personalized but discrete. It gives you *your* Google experience.

Implications

- Being clear about the roles of Guest and Incognito is important.
- It likely makes sense to offer both.

Known: Usability is a challenge

- We need to properly describe Incognito in-context, and make use transparent and understandable.
- Discoverability is also important.

Implications

- We need to design a consistent UX for Incognito that applies across platforms.

break for other presentations

Use case: Sensitive Activity

- Seeking birth control information.
- Buying a present secretly.
- Porn.

Not use case: Dangerous Domains

- Reporting war crimes from a war zone.
- Political dissident fighting established government.

Not use case: High stakes comms

- Lawyer communicating in anti-trust lawsuit.
- Corporate researcher transmitting critical intellectual property.

EXHIBIT 14

Redacted Version of Document
Sought to be Sealed

Message

From: Chris Palmer [palmer@google.com]
Sent: 2/11/2015 6:52:47 PM
To: Adrienne Porter Felt [felt@google.com]
CC: Parisa Tabriz [parisa@google.com]
Subject: Re: Incognito-fest 2015

On Wed, Feb 11, 2015 at 4:41 AM, Adrienne Porter Felt <felt@google.com> wrote:

> Second question. Is Incognito something our team wants to take on? (Palmer,
> in Q2 or Q3?) It would take attention and focus away from HTTPS but OTOH it
> is also something I know we all care about. Or should we focus on trying to
> poke the privacy team into action?

1. Sure, I can give a brief briefing. What is the best format?
Document, slides, in-person chat, a CL that has +0 lines and -15000?
:)

2a. I'm not sure we should take it on. It's radioactive: In its
current form, it is effectively a lie; in its fixed form (rebranded,
clarified) it will be a huge negative press cycle like Master Password
was (most people drunkenly screeching; Kevin Poulsen being the lone
sane voice); in its genericized form [REDACTED]

[REDACTED] people will
think we killed it unceremoniously and then it will be 100%
screeching.

2b. If we don't take it on, it will fester and perhaps metastasize,
and we will feel like we were derelict in our duty.

2c. Does Privacy team realize they have dropped the ball? I.e. if we
try to take it on, will they push back thinking it's still theirs? Or,
can we get them on board with our plan and then get them to act on it,
solving (2a)?

EXHIBIT 16

Redacted Version of Document
Sought to be Sealed

Message

From: Chris Palmer [palmer@google.com]
Sent: 11/6/2018 6:38:47 PM
To: Michael Paddon [mwp@google.com]
CC: Michael Kleber [kleber@google.com]; Mike West [mkwst@google.com]; potassium@google.com; chrome-privacy-core@google.com
Subject: Re: EFF: "Google Chrome's Users Take a Back Seat to Its Bottom Line"

We certainly do have our blind spots (hoooo boy). You're right that the culture is changing, and what was acceptable is less acceptable now; but I'm not sure EFF is necessarily the bellwether we should look to — I find e.g. Zeynep Tufekci's NYT articles a much more compelling and mainstream-understandable critique.

But whatever; what's more important is that we do something meaningful soon. I've bargled various ideas; we could also tighten the 3P cookie rules or block 3P cookies by default in Incognito. Maybe that's not a good idea for various reasons, but we could certainly ship it and things like it soon if we wanted to.

On Tue, Nov 6, 2018 at 4:13 AM Michael Paddon <mwp@google.com> wrote:

I don't think we can conclude "[REDACTED]" in general. It does in experiments where advertisers can defect to status quo. But we cannot conclude what the behaviour would be in the absence of 3p cookies from the entire ecosystem. Put another way, A/B testing is effective for gradient descent but not for finding global minima.

Just as it is easy for us to see EFF's blindspots, we should be aware that we also have enormous blindspots of our own. And so do our advertising partners.

What I see is that the world is changing. The EFF is a bellwether. What was acceptable behaviour in data gathering is becoming unacceptable. I think we need to get out ahead and own the change rather than defending old business models. If the market wants a truly incognito mode, let's give them the best one possible.

On Tue, Nov 6, 2018 at 6:36 AM, Michael Kleber <kleber@google.com> wrote:

Thanks, Chris, that does help.

Much as I love the "We should continue to reach out and offer to help inform them" point of view in general,

[REDACTED]. Even internally we hedge and point out that it's different for every site, which is true, but frankly I think this is so locked-down because we don't want to cause industry-wide panic.

Unfortunately, so long as we're unwilling to talk about this detail externally, I don't see a path to substantially changing the narrative.

--Michael

On Mon, Nov 5, 2018 at 2:16 PM Chris Palmer <palmer@google.com> wrote:

I have worked at EFF twice, first as Staff Technologist & Technology Manager, and again as Technology Director. So maybe I can provide some context. I left EFF and came to Google on the informed belief that I can successfully do more EFF-like work here than at EFF. After 7 years here, I am certain I was right. But, do take this with a grain of salt — I have A Viewpoint and it might not be 100% objective. :)

To answer Michael's question: It's ignorance, not malice. (Sure, they're feisty, but that is good!) Generally, EFF does not think hard about how people who create information goods make money. They have an old-timey Wired Magazine/1990s internet boom/techno-solutionist/"we're already post-scarcity!" ideology that requires them to believe that low marginal cost per copy means that information goods are 'free' to make. You'll see this in their positions on any information good, whether it's software, music, journalism, literature, et c. (They rely heavily on Cory Doctorow's hard-to-replicate experience of getting lucky, which notably involved running a popular ad-supported blog. Doot-de-doo...)

As for "credulous and naive", yes; part of their problem is epistemic closure. (Again, *not malice* — they are good people trying to do the right thing.) They tend to alienate people who could inform them, leaving only people who already agree. For example, they didn't ask me if they had the facts right before posting this post, despite knowing me and that I am on Chrome Security; similarly, AFAIK they have never had anyone who has ever been in the intelligence community on staff.

Their closure also reduces their potential reach, although they do have vocal support in parts of the security engineering community (and, weirdly, vocal opposition in other parts of the security community). We should continue to reach out and offer to help inform them. I don't necessarily expect huge returns from that; Google gave EFF an early view of Gmail and EFF still blasted them for its "creepiness", but I think it was good for everyone to at least have the conversation. It's better than random broadsides like this post.

Ultimately, the blame for people's misconceptions about Incognito Mode is due to that name and branding, as I have argued repeatedly. I believe the Incognito part of this blog post would basically not exist if we had called it (e.g.) Temporary Mode.

Could Incognito/Temporary work better, such as the site- or origin-specific local storage deletion? Sure, maybe that would work. As much as I want to ratchet down the brand and apparent 'guarantee', I am also in favor of ratcheting up the guarantee *where technically possible*. (I'll continue to push back on infeasible or impossible guarantees.)

On Mon, Nov 5, 2018 at 6:26 AM Michael Kleber <kleber@google.com> wrote:

I am really surprised by their never touching on how publishers get money. They (wrongly) claim that "The marginal benefit of each additional bit of information about your activities online is relatively small to an advertiser, especially given how much you directly give Google through your searches". But there is no corresponding thinking about the marginal benefit of the cookie is *huge for publishers*, because without it we have no way to bring *any* of that information to bear on display ad monetization.

Any opinion on whether that omission is ignorance or malice?

Their take on "incognito mode" is very interesting. The idea that it "does nothing to protect you from being tracked by Google" is a rational complaint if you sign into Google in incognito mode (which seems like an oxymoron to me), or if you use the same incognito session for a long time.

Have we considered an

"A sustainable Web needs to be built on consent, not subterfuge" surprises me, in that I would have expected them to be as skeptical of consent as we are. Maybe political considerations mean you can't say that publicly (yet)?

--Michael

On Mon, Nov 5, 2018 at 3:27 AM Mike West <mkwst@google.com> wrote:

Ouch. <https://www.eff.org/deeplinks/2018/11/google-chromes-users-take-back-scat-its-bottom-line>

A few things to call out:

"The closest thing it offers to 'private' browsing out-of-the-box is 'incognito mode', which only hides what you do from others who use your machine. That might hide embarrassing searches from your family, but does nothing to protect you from being tracked by Google." which is an interesting form of the "Incognito should do more" argument.

"Facebook recently announced its intention to move away from using third-party cookies to power Pixel, its third-party analytics product." is a fairly naive and credulous take on Facebook's moves in this space.

"Google could take the lead on solving this problem. Trackers are not necessary to make the Web work, and they shouldn't be necessary for Google to make lots (and lots) of money. As we noted above, Google has mountains of direct information about what you want to buy through its various services, from search to Maps to Google Play. Ads don't need to be targeted using every little bit of information about us that Google has access to via our use of its browser. A sustainable Web needs to be built on consent, not subterfuge." Apparently first-party tracking is fine.

"Google has come under fire in the past for using its power in one arena, like browsing or search, to drive revenue to other parts of its business." I heard a similar kind of argument from one of our friends at Samsung at dinner during TPAC a week or two ago.

-mike

--

You received this message because you are subscribed to the Google Groups "potassium" group.

To unsubscribe from this group and stop receiving emails from it, send an email to

potassium+unsubscribe@google.com.

To post to this group, send email to potassium@google.com.

To view this discussion on the web visit

<https://groups.google.com/a/google.com/d/msgid/potassium/CAKXHy%3Dc1Ovb%3DLbdoQeAa7r%2B9y2Kaya7G7xfmtZ3SzKKq8rOa%2BA%40mail.gmail.com>.

--

Forewarned is worth an octopus in the bush.

--

You received this message because you are subscribed to the Google Groups "potassium" group.

To unsubscribe from this group and stop receiving emails from it, send an email to

potassium+unsubscribe@google.com.

To post to this group, send email to potassium@google.com.

To view this discussion on the web visit

<https://groups.google.com/a/google.com/d/msgid/potassium/CAA6DcCePf9riuRtP%3DgO0u4RUcG6A3%2Bi%3D4Yct2tPonpAPtW0VNg%40mail.gmail.com>.

--

Forewarned is worth an octopus in the bush.

--

You received this message because you are subscribed to the Google Groups "potassium" group.

To unsubscribe from this group and stop receiving emails from it, send an email to

potassium+unsubscribe@googlegroups.com.

To post to this group, send email to potassium@googlegroups.com.

To view this discussion on the web visit

<https://groups.google.com/a/google.com/d/msgid/potassium/CAA6DcCdpq3SfjVdc7yLTZBJ7EnecZWk2XM2DnYm0rtOK718p2A%40mail.gmail.com>.

EXHIBIT 20
Redacted in its
Entirety

EXHIBIT 22
Redacted in its
Entirety

EXHIBIT 23

Redacted Version of Document
Sought to be Sealed

Message

From: Mardini [mardini@google.com]
Sent: 4/30/2019 7:14:16 PM
To: Jochen Eisinger [eisinger@google.com]; Shimi Rahim [srahim@google.com]
CC: Margret Schmidt [margrets@google.com]; Parisa Tabriz [parisa@google.com]; Alex Ainslie [ainslie@google.com]
Subject: Re: Branding for Incognito (IO Update)

[narrowing down list of recipients - pls don't forward]

An update on our meeting with Sammit today. We discussed the following:

- 1/ Debugging the process
- 2/ Got context around the incognito iconography/rebranding for I/O then cancellation
- 3/ Got clarity on who owns that Incognito comms doc and whether our comments are being addressed

1/ Made it clear what the ideal process should be from Chrome's point of view. No disagreements there and it was clear for them but there was a mad rush to get things for I/O from various execs that made folks panic.

2/ This was driven by Lorraine who told the PDPO steering committee that Incognito might need rebranding so a workstream ensued involving the brand studio about 2-3 weeks ago.

Yesterday, at the PDPO SC meeting, Tom Oliveri was present and told them that Sundar didn't want to put incognito under the spotlight so this iconography/rebranding should not be an I/O topic.

The plan of record with regards to incognito in I/O is just to mention in one or two sentences related to bringing Incognito to Google Maps (not clear whether there will be mocks or not for that).

The SC was asked to commit to exploring in 2019 to develop a consistent vision for how an "Incognito 2.0" would look like with impact analysis on revenue, usage, and comms.

Relatedly, Ben Gomes showed a demo of AGSA launching Chrome in Incognito mode. i.e. if a user is in AGSA and they want to conduct an incognito search, they'd intent into an Incognito NTP in Clank

3/ That comms doc is owned by the brand studio and Sundar's speech writing team. I emphasized the need to double check with Chrome PM/Eng the accuracy of the information mentioned there. Sammit acknowledged but mentioned that the comms around I/O are very closely guarded and it's challenging to get a full picture for what will be said exactly....

Thanks,

--Mardini

On Tue, Apr 30, 2019 at 8:40 AM Mardini <mardini@google.com> wrote:

Le mar. 30 avr. 2019 à 08:33, Mardini <mardini@google.com> a écrit :

Thank you, Alex.

We (Rory/Ramin/Sabine/myself) have a meeting with Sammit today so will discuss the process and work cadence issue as well.

As discussed in our chat yesterday, Jochen and I will try to get some time with the PDPO folks visiting Munich for GSEC in a couple of weeks to sync in person.

I also didn't receive the note below about revisiting the incognito brand after I/O. Maybe it was sent only to those who replied "yes" to the meeting.

I see it now. Gmail didn't classify it as important :/.

Le mar. 30 avr. 2019 à 07:29, Yuan Chen <yuanchen@google.com> a écrit :

Thank you for keeping us in the loop - I also didn't get the update from PDPO. I agree we need to get into a better work cadence with PDPO folks.

On Tue, Apr 30, 2019 at 2:12 AM Shimi Rahim <srahim@google.com> wrote:

Thanks for filling us in, Alex & Parisa (I didn't see an email from PDPO), and for helping us navigate I/O challenges!

On Mon, Apr 29, 2019 at 5:03 PM Parisa Tabriz <parisa@google.com> wrote:

On Mon, Apr 29, 2019 at 4:42 PM Alex Ainslie <ainslie@google.com> wrote:
(narrowing to just Chrome folks)

I'm glad to see the update from PDPO below about waiting to tackle any branding updates until After IO.

Ah, me too!

Their timing was too aggressive and their proposal wasn't compelling :/

Here's the Chrome summary from my discussions with many of you (in sequence) this morning:

- Chrome is comfortable with a high level message at IO about expanding Incognito to other flagship Google products on Android (AGSA, Maps, YouTube).
- We've nurtured the Incognito brand for the past 10 years and our team would need to conduct a significant investigation (including UX Research) to feel confident about a change.
- For that reason, Chrome does not support announcing new PDPO-proposed branding at IO
- Additionally, speculative announcements related to Privacy are extra risky because the bar for Google is high and we need to make sure not to promise something we can't deliver.

Chrome + PDPO (Mis)alignment

Should Google ...	PDPO + Brand Studio	Chrome
... do more product work focused on Privacy?	Yes	Yes
... talk more about that Privacy work in public?	Yes	Yes
... extend Chrome's Incognito mode to other products?	Yes	Maybe?
... change the current Incognito brand?	Yes	Maybe? Err
... announce Incognito branding changes at IO before they've been thoroughly studied?	Yes	No

Going forward, I agree with Jochen that we'll need to get into a better working cadence with PDPO folks.

Yep. I'd recommend syncing with miraglia@ in a small setting to share how this effort was perceived from the Chrome side so we can reset.

Alex

On Mon, Apr 29, 2019 at 4:00 PM Sammit Adhya <sadhya@google.com> wrote:

Hi Everyone,

Just wanted to let you know that leads decided to revisit the Incognito branding after I/O. Apologies for scheduling the urgent meeting, but we look forward to working with everyone after I/O.

Thanks much,

Sammit

[Confirmed] - Exploration of Iconography and Branding for Incognito

Scheduled per Sammit's request

We wanted to share some new Incognito branding and iconography ideas that the Brand Studio team has been exploring to get your thoughts and feedback.

Leads: anilsa, parisa, miraglia

PM: (rorymccllland), (sabineb), mardini

Eng: eisinger, (rhalavati)

UXR: martinshelton, (lorindole)

UXD: ainslie

Marketing: martinal, jcroom

Brand: mediha, julianneyi, frederick

PDPO: sadhya, gregfair, rast

When Tue Apr 30, 2019 3:30pm – 4pm Pacific Time - Los Angeles

Where MTV-900-2-ChromeOZone (8) [GVC, No External Guests], MTV-900-2-Rage Against The Machine (4) [GVC, No External Guests], SFO-1MST-14-Daniel Handler (4) [GVC], SFO-2HS-4-Eight O'Clock Coffee (5) [GVC], SYD-ODI-3-410 - Gone (2) [GVC, No External Guests, Phone] ([map](#))

Joining info

Or dial: + [REDACTED] [More phone numbers](#)

Who

- Eric Miraglia - organizer
- Jieun Lee - creator
- Martin Shelton
- Sammit Adhya
- rast@google.com
- Martina Laresova
- Ken Frederick
- Jochen Eisinger
- James Croom
- Anil Sabharwal
- Mediha Abdulhay
- Greg Fair
- Alex Ainslie
- Shimi Rahim
- AbdelKarim Mardini
- Martha Welsh
- Julianne Yi
- Parisa Tabriz

- Ramin Halavati - optional
- Lorin Dole - optional
- Sabine Borsay - optional
- Rory McClelland - optional

--

Yuan Chen

Interaction Designer

Google Germany GmbH

Erika-Mann-Str. 33

80636 München

Geschäftsführer: Paul Menckel, Halina Delaine Prado
Registrierungsamt und -nummer, Hamburg, HRB 88881
Sitz der Gesellschaft: Hamburg

Diese E-Mail ist vertraulich. Wenn Sie nicht der richtige Adressat sind, bitten Sie dies bitte nicht weiter, informieren Sie den Absender und löschen Sie die E-Mail und alle Anhänge. Vielen Dank.

This e-mail is confidential. If you are not the right addressee please do not forward it, please inform the sender, and please erase this e-mail including any attachments. Thanks.

EXHIBIT 24

Redacted Version of Document
Sought to be Sealed

Message

From: Jochen Eisinger [eisinger@google.com]
Sent: 3/22/2019 7:42:29 AM
To: Mike West [mkwst@google.com]; AbdelKarim Mardini [mardini@google.com]
CC: Alex Nicolaou [anicolao@google.com]; Michael Kleber [kleber@google.com]; Rick Byers [rbyers@google.com]; Rory McClelland [rorymcclelland@google.com]; Vivek Sekhar [vsekhar@google.com]
Subject: Re: Follow up from Sundar meeting

+AbdelKarim Mardini

On Fri, Mar 22, 2019 at 6:13 AM Mike West <mkwst@google.com> wrote:
 +Jochen, Rory

On Fri 22. Mar 2019 at 05:59, Alex Nicolaou <anicolao@google.com> wrote:
 Ads Team summary.

----- Forwarded message -----

From: Ben Galbraith <bgalbs@google.com>
Date: Thu, Mar 21, 2019 at 4:33 PM
Subject: Fwd: Follow up from Sundar meeting
To: Jack Chen <jlchen@google.com>, Darin Fisher <darin@google.com>, Parisa Tabriz <parisa@google.com>, Margret Schmidt <margrets@google.com>, Alex Nicolaou <anicolao@google.com>, Vivek Sekhar <vsekhar@google.com>, Ivy Choi <ivyc@google.com>, Ben Goodger <beng@google.com>
Cc: Anil Sabharwal <anilsa@google.com>

Privileged and confidential

FYI, here's the Ads team version of the note I sent out earlier.

----- Forwarded message -----

From: Struan Robertson <struan@google.com>
Date: Thu, Mar 21, 2019 at 12:54 PM
Subject: Re: Follow up from Sundar meeting
To: Chetna Bindra <cbindra@google.com>, Jack Chen <jlchen@google.com>
Cc: Jerry Dischler <jdischler@google.com>, Suresh Kumar <sureshkm@google.com>, Shiv Venkataraman <shivav@google.com>, Sagnik Nandy <sagnik@google.com>, Anurag Agarwal <anuragag@google.com>, Darin Fisher <darin@google.com>, Anil Sabharwal <anilsa@google.com>, Ben Galbraith <bgalbs@google.com>, Brad Bender <bradbender@google.com>

+Jack Chen

On Thu, Mar 21, 2019 at 12:37 PM Chetna Bindra <cbindra@google.com> wrote:
 Privileged and confidential

All,

Thanks for all the collaboration leading up to the Sundar meeting. Overall we had a positive meeting with Sundar, landing on approval for our recommendation in the deck. He acknowledged the complexity of this space and expressed his gratitude on the progress we've made given the complex topic. He specifically said that we do not need to come back for a review, but he would review comms in the lead up to I/O.

Key takeaways

- Totally agreed with the strategic value of balancing both ecosystem health and privacy
- Overall comfortable with not removing 3P cookies, but wanted to focus on how Chrome is helping users with 3P cookie concerns (i.e., "3P cookies" have become a strong industry narrative that we can't ignore or wait years to address). He was supportive of our plans to address these issues largely with opt-in controls that we should make sure are incorporated as part of our messaging at I/O.
- Overall approval of plan on data disclosures, Ads Privacy center, Chrome guard controls - 3P / Incognito controls
- Focus on messaging by I/O. Ensure it covers the entire proposal - data disclosures, Ads privacy center, Chrome controls, data retention within Chrome and Ads. A lot of enthusiasm for "[REDACTED]" and encouragement to dovetail with the broader Google Incognito narrative if we're ready.
 - (A tactical AI was given to the Chrome team to dovetail with a broader data retention initiative.)
- Comfortable with reactive messaging on saying that Apples 3P cookies removal hasn't done enough, and 3P tracking continues
 - Sundar drove the point in the meeting (with several other examples) that if Chrome removes 3P cookies, it would create a very disruptive situation for publishers, and is keen to support overall ecosystem health. He acknowledged that Apple and Google are optimizing for different things.
- He firmly expressed a desire for both Chrome and Ads to get out in public with a narrative ASAP. He felt that silence in the market was no longer an option, and alignment that I/O was the right initial moment, followed by GML
- Eventual enforcement seemed to be a punted question

Key AIs / Next Steps

Evaluate an advisory board rather than a coalition, and learn from the AI advisory board
 Plug in with the I/O and GML team for messaging

Best,
 Chetna (on behalf of the team)

Struan Robertson | Director, Legal | struan@google.com | 650-713-7613

This email may be confidential or privileged. If you received this communication by mistake, please don't forward it to anyone else, please erase all copies and attachments, and please let me know that it went to the wrong person. Thanks.

--
 -mike

EXHIBIT 25
Redacted in its
Entirety

EXHIBIT 26

Redacted Version of Document
Sought to be Sealed



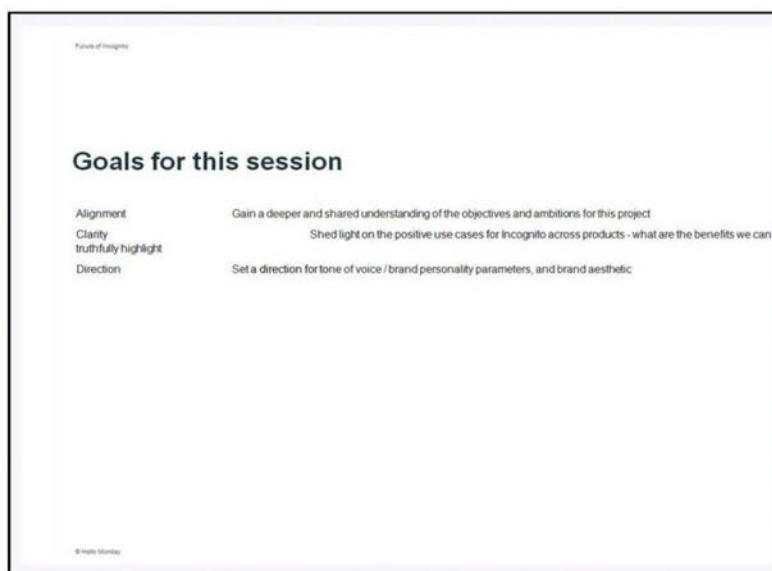
Future of Insights

Agenda

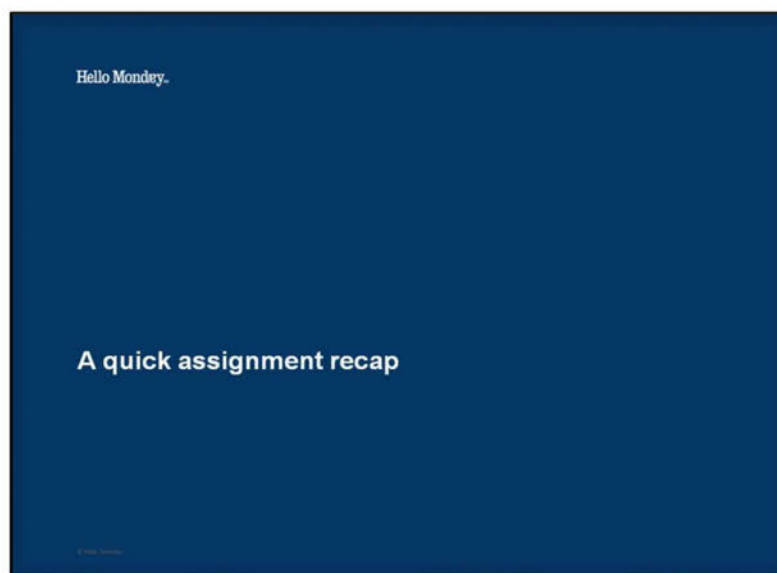
– Quick introduction (name/role)	5 min
– Workshop goals	5 min
– Recap of the project brief (Sammit)	15 min
– Top use cases discussion	25 min
– Brand wheel discussion	20 min
– Onlyness exercise discussion	5 min
– What does success look like?	
– Next steps	

© 2020 Sammit

20-25 min buffer



20-25 min buffer



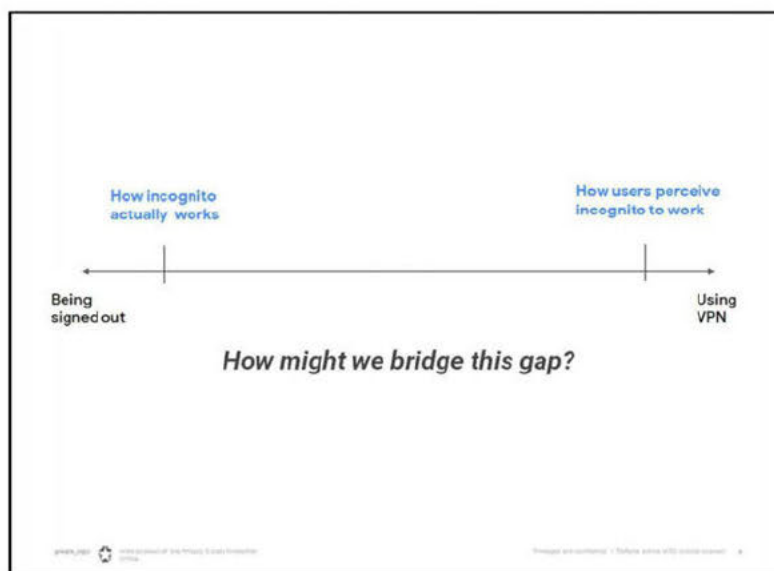
Design a clearly branded, well-defined Incognito experience where the ability to activate and deactivate this mode is **trivially simple, intuitive** and **consistent** across our products.

Design a comprehensive **messaging strategy** that helps users understand how incognito works and how to appropriately use it to match its functionality.

© 2022 Google LLC. All rights reserved. Privacy Policy

Incognito is a trademark of Google LLC. All rights reserved.

Communication of incognito means



What's Incognito?


.... probably not what you thought.

Incognito will delete:

- cookies
- browsing history
- Temp files/cache
- Form data

Incognito will not:

- Delete downloaded files
- Obscure IP/location
- Obscure device from internet



You've gone incognito


Now you can browse privately and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. [Learn more](#)

Chrome **won't** save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might** still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

chrome://incognito/  Some portions of this Privacy & Security information may be hidden.

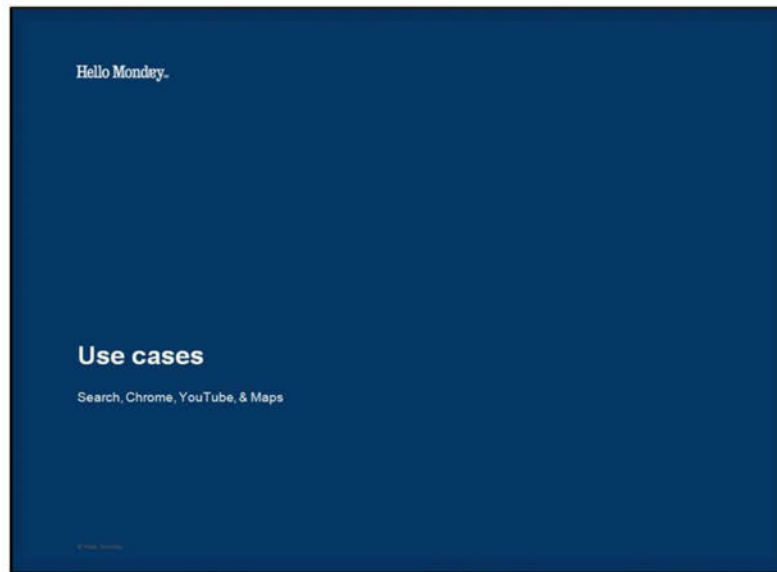
Privacy and security > Settings > chrome://incognito/ 1 / 8

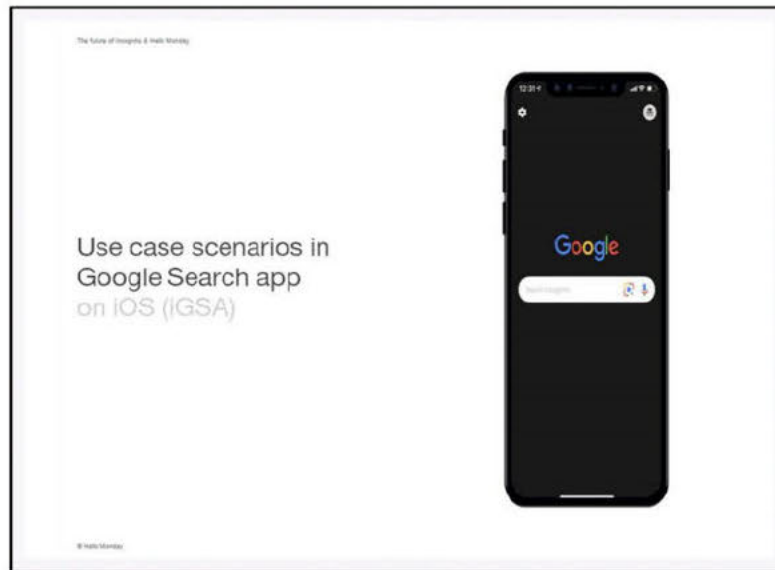
Analogy #1

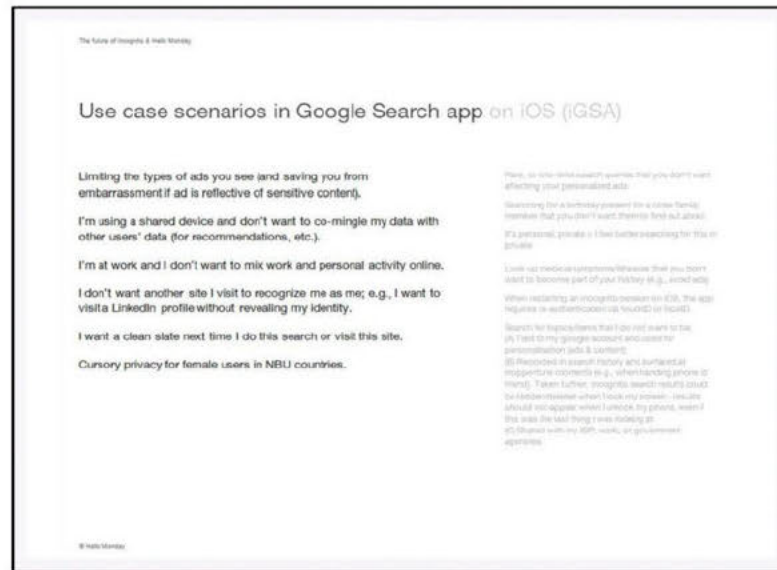
What is Incognito?

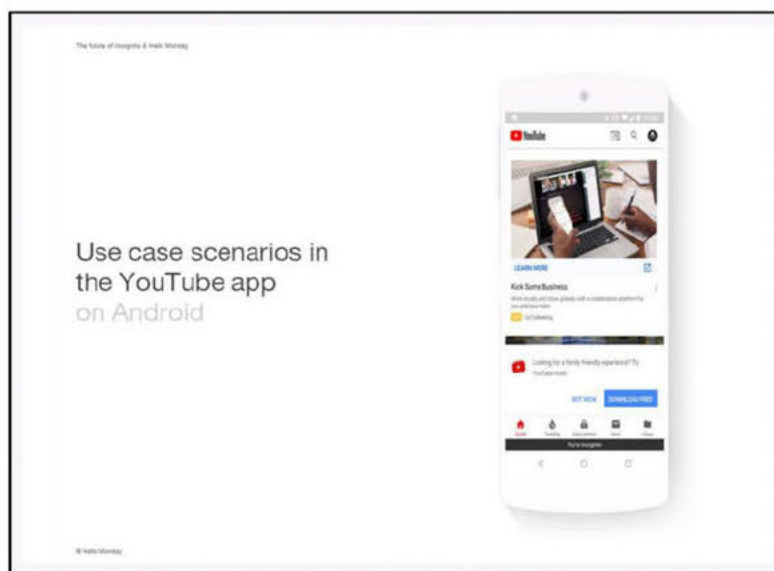
It's like not getting your passport stamped when you go on holiday. Anyone looking at your passport will have no idea you've been to Jamaica. But the Jamaican authorities will know you've been, as will the airline. And that loud shirt you brought back gives the game away.











The Future of Incognito & Make Moments

Use case scenarios in the YouTube app on Android

Let my little nieces and nephews watch their kiddie videos that I don't want to see again

Learning how to do something new and ambitious like exploring a new business, entrepreneurship, where you don't want to let anyone else know about it yet.

Searches & content you wish to keep private from family on a shared device in a NBU country.

Incognito especially helps reduce the potential that ephemeral or one-time interests don't take over your video recommendations.

When I watch or search for videos in incognito, I do not want them to be surfaced at inopportune moments (e.g., when handing phone to friend). * Therefore, incognito videos should be hidden/deleted when I lock my screen or press the power button. - video should not appear when I unlock my phone, even if this was the last thing I was looking at.

Incidentally, keeping the videos in a private, secure space where users who have concerns about their privacy within their household can use the phone without being worried to share access to them.

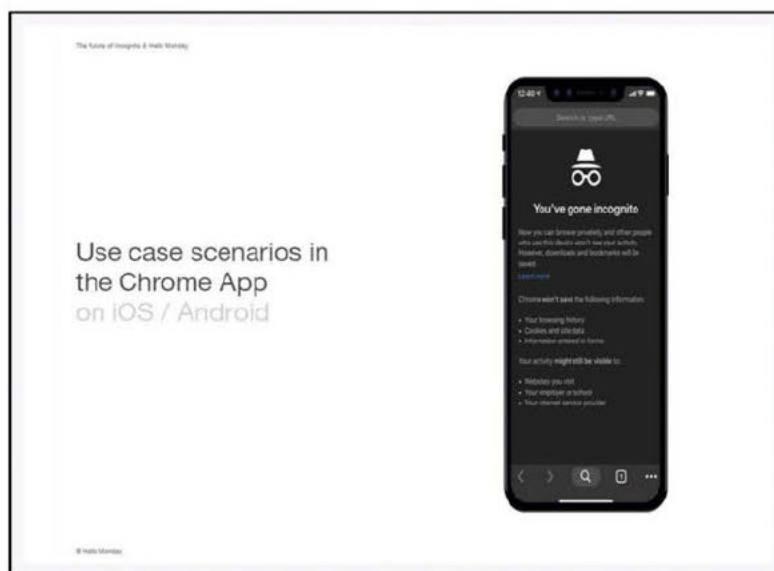
Prevent data generated during a "YouTube session" from being logged, locally or on the server, to prevent the data being used for personalization or ad targeting.

but impacting recommendations with specific types of content.

YouTube personalization heavily favors recency - i.e. videos that you watched in the last few hours will influence your recommendations more than videos you watched a long time ago. Incognito especially helps reduce the potential that ephemeral or one-time interests don't take over your video recommendations.

* Great idea! Let's make sure this is followed up upon as a product feature.

© Make Moments



The future of Incognito & Private Browsing

Use case scenarios in the Chrome app on iOS / Android

Being anonymous on shared docs (Spreadsheets, Google Docs)

Checking out someone's LinkedIn/ Facebook Profile anonymously

Checking Public Links if you are the owner / creator

Things you don't want in your search history

* When I am browsing in Incognito, I am primarily doing so to protect my local privacy. Therefore, Incognito browsing should be hidden/deleted when I lock my screen or press the power button - it should not reappear when I unlock my phone, even if this was the last thing I was looking at.

On Android, incognito always notifies you to close all incognito tabs (via notifications).

Getting incognito pages to not show up in search history.

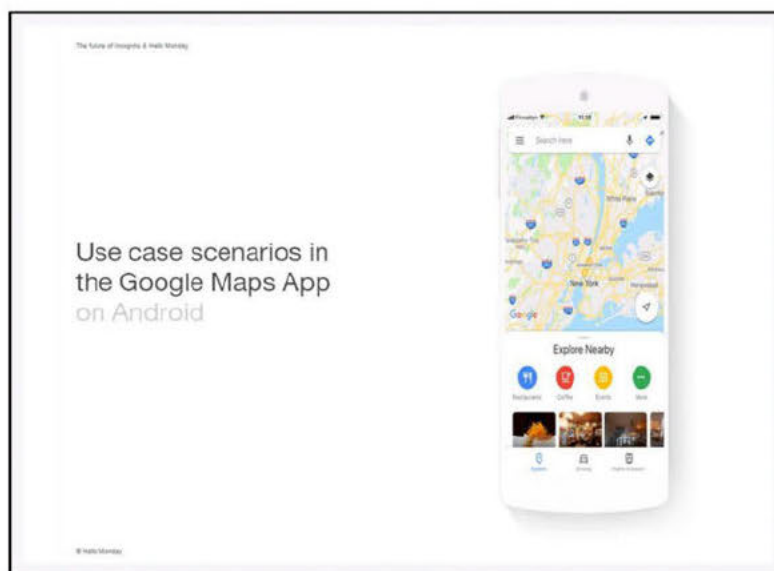
Enabling multiple user accounts if/when product open (e.g. email).

Spreadsheets are disabled when in Incognito on Android.

I don't want Chrome to plan my bookmarks and recommendations for the day I visit.

* Great idea! Let's make sure this is followed up upon as a product feature.

© 2020 Google



The future of insights & mobile strategy

Use case scenarios in the Google Maps app on Android

Visit to Planned Parenthood (from the recent New York Times article on location tracking)

I might use Incognito to remove personalisation - I would like to see restaurants, shops, and events that are not surfaced on the basis of my location history or stated preferences.

Finding a gift, or location for a party without others finding out about it (like when its for a surprise)

At-risk users — for example, sufferers of stalking or domestic abuse — might want to obscure their location history

*Potential to use maps without location leaving the device (though it has not been built yet).

We discuss on recommendations in "How You" tab:
I don't want Google to personalize the places I am going. I know these places already and I don't want them cluttering up my Maps experience

*Great idea! Let's make sure this is followed up upon as a product feature.

© 2020 Google

The Future of Incognito & Private Mode

Takeaway - interesting themes in use cases

Control - Not so much of Incognito experience, but more of the 'normal mode' experience.
Avoiding pollution of 'normal' mode experience by having one-time searches influence ads and content suggestions.
Avoid mingling work activity with private activity.

Device Sharing - Keeping searches away from others' eyes
Children + Households: Going Incognito when devices are shared with kids or out of courtesy to others in the house.
Or to avoid spoiling surprises and having embarrassing results pop up.

Site-specific - Being 'anonymous' on a certain site for very specific reasons
LinkedIn profile searches, Google docs, checking public sites when you're the owner.

NBU - Incognito is proving relevant here - cultural considerations
Device sharing is common. ███% of Indian women borrow a device for primary access. ████ share their device at least once a month. *

© 2019 Google

The future of Incognito & Hello Monday

Our task in a nutshell



© Hello Monday

Analogy #2

What is Incognito?

It's like speaking to a journalist off the record.
*It protects your anonymity up to a point, but it
doesn't mean the conversation never happened.*



EXHIBIT 28
Redacted in its
Entirety

EXHIBIT 28
Redacted in its
Entirety

EXHIBIT 30

Redacted Version of Document
Sought to be Sealed

Message

From: Rory McClelland [rorymcclelland@google.com]
Sent: 2/6/2020 3:56:43 PM
To: Christian Dullweber [dullweber@google.com]
CC: Ramin Halavati [rhalavati@google.com]; Angel Maredia [angelsm@google.com]
Subject: Re: Chrome Incognito Metrics

Thanks, both!

On Thu, 6 Feb 2020 at 02:27, Christian Dullweber <dullweber@google.com> wrote:
[REDACTED] % of users used the Clear Browsing Data dialog in the last 28 days. [REDACTED] % deleted cookies at least once.
[REDACTED]

On Wed, 5 Feb 2020 at 22:57, Ramin Halavati <rhalavati@google.com> wrote:
+Christian Dullweber

Hi Angela,

Based on this query, in the last 28 days, in US, and on Android and iOS, we had [REDACTED] unique users of incognito mode and [REDACTED] of regular mode. Assuming that all users of incognito mode have also used regular mode, the ratio will be [REDACTED] %.

On the clear browsing data question, Christian should know better.
Please let me know if I could help more.

Best,
Ramin

On Wed, Feb 5, 2020 at 9:49 AM Rory McClelland <rorymcclelland@google.com> wrote:
Hi Angela,

+Ramin Halavati our Incognito lead to help me out with the two questions. Thanks, Ramin.

Rory

On Wed, 5 Feb 2020 at 07:18, Angel Maredia <angelsm@google.com> wrote:
Also sorry for the follow up email! I was wondering, do you know what % of Chrome users clear their cookies or history on mobile and how often?

On Tue, Feb 4, 2020 at 10:08 PM Angel Maredia <angelsm@google.com> wrote:
Hey Rory,

My name is Angel and I'm the PM on Fi leading our privacy and security team. I was looking into Incognito mode for Chrome, and I was wondering, what % of users use Incognito mode on mobile out of total users, focusing on the US?

Thanks,

Angel

EXHIBIT 31

Redacted Version of Document
Sought to be Sealed

Steve Hamilton <sthamilton@google.com>

What we know about Incognito users (re. The most underused Privacy Surface)

7 messages

Steve Hamilton <sthamilton@google.com>

Wed, Jan 27, 2021 at 1:41 PM

To: leathern@google.com, Othar Hansson <othar@google.com>, Mark Risher <risher@google.com>, Rahul Roy-Chowdhury <rahulrc@google.com>, Sarah Hammond <shammond@google.com>, Lauren Palmer <laurenpalmer@google.com>, Gretchen Gelke <ggelke@google.com>, Arne de Booij <adebooij@google.com>, Tal Herman <talherman@google.com>, Guemmy Kim <guemmy@google.com>, Kalle Buschmann <kallebu@google.com>

Hi Everyone,

I'm Steve, a UXR in the PDPO working on Sin Rastro (Google-wide Incognito mode).

Attached is a deck that summarizes what we know about Incognito users, what they use it for, and some of the risks that we've identified over the course of the project.

It's worth noting that the Chrome team have done some excellent work in this space (as you might expect), and are putting together some very interesting plans in go/incognito2021 (slides 24 to 31 are probably the most relevant)

Please feel free to reach-out with any questions or concerns, I'm more than happy to help.

Best,

Steve

TL;DR of the deck:

Executive Summary

- Frequency of Use:
 - Incognito mode is used by █ % of Chrome users, and █ % use it at least once per week
- User Characteristics:
 - Weekly users are more likely to be █
 - 47% of weekly users state, "I do everything I can to protect my privacy," implying that they are more privacy sensitive than non-users, and may be more open to other privacy controls
- Top use cases for Incognito mode:
 - █
 - █
- Risks to press cycles on Incognito mode:
 - Users overestimate the protections that Incognito provides and are unaware of the personalization and data collection that occurs when it is on
 - When considered together, Incognito mode appears to negatively impact user sentiment towards regular browsing
 - Educational moments intended to reassure and inform users of quality-of-life features (autofill & autocomplete) have led to negative reactions

Rob Leathern <leathern@google.com>

Wed, Jan 27, 2021 at 3:47 PM

To: Steve Hamilton <sthamilton@google.com>, Annie Klemp <annieklemp@google.com>, Sam Heft-Luthy <heftluthy@google.com>, Ane Fabo Aranzabal <anefabo@google.com>
 Cc: Othar Hansson <othar@google.com>, Mark Risher <risher@google.com>, Rahul Roy-Chowdhury <rahulrc@google.com>, Sarah Hammond <shammond@google.com>, Lauren Palmer <laurenpalmer@google.com>, Gretchen Gelke <ggelke@google.com>, Arne de Booij <adebooij@google.com>, Tal Herman <talherman@google.com>, Guemmy Kim <guemmy@google.com>, Kalle Buschmann <kallebu@google.com>

Thanks Steve, appreciate the update. Will let you know any questions as we dig into the data/insights.

@Annie Klemp / @Ane Fabo Aranzabal / @Sam Heft-Luthy for context.
 Rob

[Quoted text hidden]

Sarah Hammond <shammond@google.com>
 To: Steve Hamilton <sthamilton@google.com>

Wed, Jan 27, 2021 at 5:43 PM

Thanks so much, Steve!

[Quoted text hidden]

--

Sarah Hammond | UX Director, User and PDPO | shammond@google.com |
Sign up for my office hours: go/shammond-oh

Steve Hamilton <sthamilton@google.com>
 To: Sarah Hammond <shammond@google.com>

Thu, Jan 28, 2021 at 8:25 AM

No worries, Sarah! I appreciate being asked to contribute :)

[Quoted text hidden]

Othar Hansson <othar@google.com>

Thu, Feb 4, 2021 at 5:16 PM

To: Rob Leathern <leathern@google.com>, Micha Segeritz <mseg@google.com>
 Cc: Steve Hamilton <sthamilton@google.com>, Annie Klemp <annieklemp@google.com>, Sam Heft-Luthy <heftluthy@google.com>, Ane Fabo Aranzabal <anefabo@google.com>, Mark Risher <risher@google.com>, Rahul Roy-Chowdhury <rahulrc@google.com>, Sarah Hammond <shammond@google.com>, Lauren Palmer <laurenpalmer@google.com>, Gretchen Gelke <ggelke@google.com>, Arne de Booij <adebooij@google.com>, Tal Herman <talherman@google.com>, Guemmy Kim <guemmy@google.com>, Kalle Buschmann <kallebu@google.com>

+Micha Segeritz also

[Quoted text hidden]

Micha Segeritz <mseg@google.com>
 Cc: Steve Hamilton <sthamilton@google.com>

Thu, Feb 4, 2021 at 6:34 PM

Hi Steve (just.you),

Where does this come from: Incognito mode is used by █% of Chrome users, and █% use it at least once per week (i don't have access.to the deck).

It's a lot higher than what I would have assumed based on inspecting the chrome client data.

Thanks,

Micha

[Quoted text hidden]

Steve Hamilton <sthamilton@google.com>

Fri, Feb 5, 2021 at 11:48 AM

To: Micha Segeritz <mseg@google.com>

Hi Micha,

You should have access to the summary deck now. The stats are self-reported from our Incognito survey. I agree, it does seem high given what Chrome report. I think it's a combination of self-report biases (mis-remembering/overestimating frequency of use) and the fact that Chrome use [REDACTED] cookie age as the indicator of Incognito usage (this was their method last time I heard - they may have a new metric now). This may underestimate those who stay in Incognito forever and/or have very long Incognito sessions as they would be classified as signed-out users.

It does also seem to align with some of the work that Florian has done on Chrome - good discussion amongst them in this doc.

LMK if you want to chat more,

Steve

[Quoted text hidden]

EXHIBIT 32

Redacted Version of Document
Sought to be Sealed

CONFIDENTIAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION
- - - - - x
CHASOM BROWN, ET AL.
Plaintiffs
vs. CA No. 20-cv-03664-LHK
GOOGLE, LLC
Defendant
- - - - - x

C O N F I D E N T I A L

ALL PARTICIPANTS APPEARING VIA ZOOM

VIDEO DEPOSITION of MICHAEL KLEBER
Friday, January 14, 2022 - 9:03 a.m.

Job no. 5027840
Reporter: Jill K. Ruggieri, RPR, RMR, FCRR, CRR
Pages 1 - 213

1 APPEARANCES :

2
3 Susman Godfrey LLP

4 Alexander P. Frawley, Esq.

5 1301 Avenue of the Americas, 32nd Floor

6 New York, New York 10019

7 212.729.2044

8 afrawley@susmangodfrey.com

9 - and -

10 Boies Schiller Flexner LLP

11 Beko Reblitz-Richardson, Esq.

12 Erika Nyborg-Burch, Esq.

13 44 Montgomery Street, 41st Floor

14 San Francisco, California 94104

15 415.293.6800

16 brichardson@bsfllp.com

17 enyborg-burch@bsfllp.com

18 Counsel for plaintiffs

CONFIDENTIAL

1 Quinn Emanuel Urquhart & Sullivan LLP

2 Andrew H. Schapiro, Esq.

3 Teuta Fani, Esq.

4 191 N. Wacker Drive, Suite 2700

5 Chicago, Illinois 60606

6 312.705.7400

7 andrewschapiro@quinnemanuel.com

8 teutafani@quinnemanuel.com

9 Counsel for defendant

10
11 Simmons Hanly Conroy

12 An Truong, Esq.

13 112 Madison Avenue, 7th Floor

14 New York, New York 10016-7416

15 212.257.8482

16 atruong@simmonsfirm.com

17 Counsel for plaintiffs in the Calhoun v. Google
18 matter

19
20 Also present: Toni Baker

21
22 Videographer: Bob Giannini

23
24
25
Page 3

CONFIDENTIAL

I N D E X

WITNESS:

MICHAEL KLEBER

Examination by Mr. Frawley 7

E X H I B I T S

Exhibit 1	Email, Kleber to Nicolaou,	21
	11/6/2018	
Exhibit 2	Email, McClelland to Kleber,	32
	11/7/2018	
Exhibit 3	██████████ leads notes	42
Exhibit 4	Group chat, 8/22/2019	53
Exhibit 5	Google Keyword post by	55
	Schuh, 8/22/2019	
Exhibit 6	Chat, Kaustubha and Kleber,	61
	3/20/2020	
Exhibit 7	Group chat, 8/10/2018	65
Exhibit 8	Group chat, 9/11/2018	75
Exhibit 9	"Potential Sundar Questions"	95
Exhibit 10	Notes	115
Exhibit 11	Group chat, 9/12/2019	120
Exhibit 12	Email, Schuh to Rahim,	126

Page 4

CONFIDENTIAL

1		9/13/2019	
2	Exhibit 13	"Assessing Chrome/Ads	131
3		Relationship" (Draft)	
4	Exhibit 14	"Assessing Chrome/Ads	135
5		Relationship"	
6	Exhibit 15	"K-API defaults in Chrome	140
7		Incognito"	
8	Exhibit 16	Privacy Sandbox initiative	155
9		overview presentation	
10	Exhibit 17	Group chat, 1/14/2021	171
11	Exhibit 18	Group chat, 9/5/2018	173
12	Exhibit 19	Group chat, 9/6/2018	183
13	Exhibit 20	Email, Sekhar to Kleber,	189
14		2/27/2019	
15	Exhibit 21	Email, Kleber to Jun,	190
16		2/27/2019	

CONFIDENTIAL

P R O C E E D I N G S

THE VIDEOGRAPHER: Good morning.

We are on the record. This is the videographer speaking, Bob Giannini, with court reporter, Jill Ruggieri, with Veritext Legal Solutions.

Today's date is January 14, 09:03:01
2022, and the time is 9:03 a.m. 09:03:03

We are here to take the remote 09:03:09
video deposition of Michael Kleber in the 09:03:10
matter of Chasom Brown v. Google LLC. 09:03:13

Will counsel please introduce 09:03:18
themselves for the record. 09:03:20

MR. FRAWLEY: Good morning. 09:03:21
Alexander Frawley from Susman Godfrey for the 09:03:21
plaintiffs. With me are my colleagues, Beko 09:03:26
Reblitz-Richardson and Erika Nyborg-Burch, from 09:03:28
Boies Schiller Flexner. 09:03:33

MR. SCHAPIRO: Good morning. 09:03:34
I'm Andrew Schapiro for Google. I am joined by 09:03:35
my colleague, Teuta Fani, and also an attorney 09:03:40
from Google, Toni Baker. 09:03:45

MS. TRUONG: And good morning, 09:03:46
everyone. An Truong, Simmons Hanly Conroy, on 09:03:47
behalf of plaintiffs in the Calhoun v. Google 09:03:51

CONFIDENTIAL

1 matter, which is related to this case and 09:03:54
2 appearing pursuant to the court's cross-use 09:03:55
3 order. Thank you. 09:03:58
4 THE VIDEOGRAPHER: Okay. Thank 09:04:00
5 you. 09:04:00
6 Will the court reporter please 09:04:01
7 swear in the witness. 09:04:03
8 09:04:04
9 MICHAEL KLEBER, a witness having 09:04:04
10 been duly sworn, on oath deposes and says as 09:04:04
11 follows: 09:04:04
12 09:04:04
13 EXAMINATION 09:04:04
14 BY MR. FRAWLEY: 09:04:18
15 Q Good morning, Mr. Kleber. 09:04:21
16 A Good morning. 09:04:23
17 Q Can you please state your full name? 09:04:24
18 A Sure. My name is Michael Kleber. 09:04:27
19 Q And have you testified before? 09:04:32
20 A I have. 09:04:34
21 Q When have you testified before? 09:04:37
22 A A previous lawsuit against Google. 09:04:45
23 Q And was it for a deposition? 09:04:48
24 A Yes. 09:04:51
25 Q And did you also testify for trial? 09:04:53

CONFIDENTIAL

1 Q And if you know, what did he mean by 09:45:06
2 "blocking third-party cookies by default in 09:45:08
3 incognito mode"? 09:45:11

4 A That seems to refer to the way 09:45:17
5 incognito mode in Chrome actually works today. 09:45:20

6 Q Today, does all of Chrome block 09:45:26
7 third-party cookies by default, or is it just 09:45:30
8 incognito mode? 09:45:34

9 A Just incognito mode. 09:45:35

10 Q What's a third-party cookie? 09:45:37

11 A That's a good question. 09:45:44

12 Cookies are a form of data 09:45:52
13 storage that exists in web browsers where the 09:45:58
14 browser retains some data that came from the 09:46:05
15 server and then sends it back to that server 09:46:07
16 later. 09:46:10

17 Third-party cookies are 09:46:12
18 cookies -- the phrase "third-party cookies" is 09:46:15
19 a little ambiguous and not always used to mean 09:46:24
20 exactly the same thing. But probably the best 09:46:26
21 definition of it is cookies where the server 09:46:31
22 that sent or received back the data that I 09:46:34
23 referred to is not the same as the server that 09:46:39
24 a person browsing the web is in the middle of 09:46:47
25 visiting at the time that the communication 09:46:50

Page 34

CONFIDENTIAL

1 happens. 09:46:52

2 Q And then how is that different from a 09:46:56

3 first-party cookie? 09:46:58

4 A First-party cookie is where the 09:47:00

5 server -- the domain that is sending or 09:47:03

6 receiving the cookie is the same as the one 09:47:07

7 that the person browsing is in the middle of 09:47:11

8 visiting. 09:47:18

9 Q And did you ever follow up with 09:47:22

10 Mr. McClelland about his consideration of the 09:47:23

11 idea that he mentioned? 09:47:26

12 A I don't recall. Sorry. 09:47:29

13 Q Do you know why Google chose not to 09:47:37

14 implement that idea for incognito mode? 09:47:39

15 MR. SCHAPIRO: Objection. 09:47:41

16 Foundation. 09:47:41

17 A As I think I said before, this was 09:47:49

18 not a proposal or a well-fleshed-out idea, 09:47:52

19 even. It was just a question of have we ever 09:47:59

20 thought about doing something like that. 09:48:01

21 So any question about whether to 09:48:07

22 actually pursue it or not would need to start 09:48:09

23 with an actual "it" that we might or might not 09:48:12

24 pursue, and I don't have any such particular 09:48:15

25 proposal to consider or even look at here. 09:48:18

Page 35

CONFIDENTIAL

1	page.	15:00:36
2	A Just a minute. Let me read through	15:00:39
3	to get context.	15:00:43
4	(The deponent read the	15:00:51
5	document.)	15:00:51
6	Yup, okay.	15:00:52
7	Q Do you see near the middle where you	15:00:54
8	wrote: "Seems that the Ads blog post later	15:00:56
9	this month is going to say that we get back	15:00:58
10	greater than ■ percent of advertiser CPD using	15:01:01
11	FLoC instead of third-party cookies for	15:01:05
12	in-market audience targeting"?	15:01:08
13	A Yes, I do.	15:01:11
14	Q And CPD refers to conversions per	15:01:13
15	dollar?	15:01:16
16	A That's correct.	15:01:19
17	Q And then right underneath, do you see	15:01:20
18	where you wrote: "That will make people sit up	15:01:22
19	and pay attention"?	15:01:24
20	A Yes, I do.	15:01:27
21	Q Why did you think that that would	15:01:29
22	make people sit up and pay attention?	15:01:32
23	A I think the context here is the	15:01:37
24	comment from Justin Schuh immediately above the	15:01:41
25	one that you read, in which Justin says, "I	15:01:46

Page 172

CONFIDENTIAL

1 feel like the industry is kinda sleeping on 15:01:49
2 FLoC." The FLoC API idea had been announced 15:01:53
3 sometime previously, but it had not gotten 15:02:05
4 substantial attention from the ad tech industry 15:02:10
5 at the point that this chat happened. 15:02:15
6 Q All right. I'm going to introduce 15:02:28
7 another exhibit. 15:02:29
8 (Exhibit 18 marked for 15:02:30
9 identification.) 15:02:30
10 BY MR. FRAWLEY: 15:02:30
11 Q I have to move the exhibit box thing, 15:03:04
12 which is fun but annoying. 15:03:06
13 I've introduced what's marked as 15:03:09
14 Exhibit 18. It's Bates No. GOOG-CABR-00801283. 15:03:11
15 A Okay. I have it. 15:03:20
16 Q Look at the second page. 15:03:39
17 A Just a minute. Let me read through 15:03:43
18 to get context. 15:03:45
19 (The deponent read the 15:03:57
20 document.) 15:03:57
21 Okay. Sure. 15:04:05
22 Q Okay. 15:04:09
23 Do you see where Mike West 15:04:09
24 wrote: "I see. I suppose that maps to things 15:04:11
25 like GA as well, which might be happy to accept 15:04:14

CONFIDENTIAL

1 a hashed variant of the first-party identifier 15:04:17
2 in order to do analytics"? 15:04:20
3 A Yes, I see that. 15:04:25
4 Q GA refers to Google Analytics, 15:04:26
5 correct? 15:04:28
6 A Yes, that's correct. 15:04:31
7 Q And then do you see where you 15:04:33
8 responded: "Right, great example, this is 15:04:34
9 exactly the way Google Analytics uses the 15:04:37
10 first-party cookie space today"? 15:04:39
11 Can you explain how Google 15:04:47
12 Analytics uses the first-party cookie space at 15:04:47
13 that point in time, November -- sorry, 15:04:53
14 September 2018? 15:04:55
15 MR. SCHAPIRO: Objection. 15:04:56
16 Foundation. 15:04:56
17 A Yes. So Google Analytics is a -- an 15:05:08
18 analytics service that lets website owners 15:05:10
19 understand some kind of aggregated information 15:05:24
20 about how people use their website. Obtaining 15:05:29
21 that information requires -- is built on Google 15:05:42
22 Analytics understanding not just one individual 15:05:50
23 page load at a time, but understanding like a 15:05:57
24 whole session -- a whole sequence of page view 15:06:01
25 kind of activity that might happen on one site 15:06:07

CONFIDENTIAL

1 at a time. 15:06:13

2 And stitching together those 15:06:16

3 individual page views into an overall session 15:06:23

4 on one particular website requires having some 15:06:26

5 sort of pseudonymous identifier that is 15:06:33

6 associated with all of those individual page 15:06:37

7 loads. 15:06:42

8 So that -- the way in which 15:06:44

9 Google Analytics uses the first-party cookie 15:06:49

10 space as described in this chat is exactly to 15:06:54

11 store the pseudonymous identifier that is 15:06:58

12 associated with one browser's behavior on one 15:07:04

13 particular website. 15:07:08

14 Q And you mentioned just a moment ago 15:07:15

15 something about stitching together those 15:07:17

16 individual page views. 15:07:20

17 Does Google Analytics use 15:07:21

18 cookies to do that stitching? 15:07:23

19 A Yes. 15:07:31

20 Q And would those be first-party 15:07:32

21 cookies or third-party cookies? 15:07:33

22 A First-party cookies. 15:07:37

23 Q So if a user visits a website that 15:07:40

24 uses Google Analytics, like The New York Times, 15:07:43

25 for example, the New York -- sorry, the 15:07:47

Page 175

CONFIDENTIAL

1 analytics cookie will be first-party cookie? 15:07:50

2 A This is somewhat confusing, actually. 15:07:58

3 As -- yeah. 15:08:07

4 Yeah. First-party cookies on 15:08:20

5 The New York Times's website are cookies that 15:08:31

6 are available when you're on New York Times or 15:08:39

7 when your browser is communicating with New 15:08:45

8 York Times. 15:08:48

9 If your browser is communicating 15:08:52

10 with New York Times, then the cookies are sent 15:08:54

11 to the server as part of the request, or at 15:09:03

12 least they might be in some cases. 15:09:05

13 If you're looking at a webpage 15:09:09

14 on The New York Times website, then The New 15:09:14

15 York Times cookies can also be accessed by -- 15:09:20

16 or some New York Times cookies can also be 15:09:24

17 accessed by the JavaScript code that is part of 15:09:28

18 The New York Times's website. 15:09:34

19 All of those things that I just 15:09:41

20 described are first-party cookies. And that 15:09:44

21 type of first-party cookie that is accessed 15:09:53

22 through JavaScript that is built into The New 15:09:59

23 York Times's website is the way in which Google 15:10:03

24 Analytics uses first-party cookies to -- to get 15:10:08

25 a pseudonymous identifier associated with 15:10:18

Page 176

CONFIDENTIAL

1 multiple different page views on New York 15:10:22
2 Times. 15:10:25

3 Q So do you recall earlier where you 15:10:30
4 said that today, Chrome, by default, blocks 15:10:31
5 third-party cookies within incognito? 15:10:35

6 A Yes. 15:10:39

7 Q So blocking third-party cookies by 15:10:41
8 default within incognito has no effect on the 15:10:43
9 Google Analytics processes you just described, 15:10:45
10 correct? 15:10:48

11 A I believe that's correct, yes. 15:10:52

12 Q Does blocking third-party cookies by 15:10:57
13 default have any effect on Google Analytics? 15:10:59

14 A I'm not sure. 15:11:07

15 Q And within an incognito session, 15:11:14
16 let's say on New York Times, the cookie is 15:11:17
17 being sent back and forth, does Chrome save 15:11:22
18 those cookies? 15:11:25

19 MR. SCHAPIRO: Objection to the 15:11:26
20 form of the question. Vague. Ambiguous. 15:11:26

21 A I'm sorry, could you repeat the 15:11:30
22 question? 15:11:32

23 Q Yes. 15:11:32

24 So I just want to go back to -- 15:11:33
25 we were talking about The New York Times, 15:11:37

EXHIBIT 34

Redacted Version of Document
Sought to be Sealed

Message

From: Justin Schuh [jschuh@google.com]
Sent: 8/30/2016 7:22:59 PM
To: Mike West [mkwst@google.com]
CC: Jochen Eisinger [eisinger@google.com]; Ojan Vafai [ojan@google.com]; Dominic Battre [battre@google.com]; Joel Weinberger [jww@google.com]; Artur Janc [aaj@google.com]; chrome-security-owp [chrome-security-owp@google.com]; Stephen Röttger [sroettger@google.com]
Subject: Re: HEIST is a good reason to revisit third-party cookie handling?

This is similar to where mixed-content blocking was several years ago. Microsoft had a very dodgy implementation, but at least they were doing something. And their work gave us cover when we started attacking the problem, and iterated on increasingly better blocking.

Eventually, other browsers started tagging along, and some sucker even got duped into making a spec out of it. ☹

On Tue, Aug 30, 2016 at 12:04 PM, Mike West <mkwst@google.com> wrote:

On Tue, Aug 30, 2016 at 8:40 PM, Jochen Eisinger <eisinger@google.com> wrote:
 Safari moving the needle? o_O

Perception-wise, totally. And their default is stricter than ours.

What they call third-party cookie blocking is not really blocking. I'd be fine with making our default to do what Safari does (only block writing if there are no pre-existing cookies), but keep our "block 3rd party cookies" setting as is (actually block stuff).

SGTM as a first step, but, you know, let's break all the things.

On Tue, Aug 30, 2016 at 6:23 PM Mike West <mkwst@google.com> wrote:
 +ojan, who I thought was added earlier in the thread, but apparently wasn't.

On Tue, Aug 30, 2016 at 5:59 PM, Justin Schuh <jschuh@google.com> wrote:

I totally appreciate the compatibility concerns, but Safari has been moving the needle here for several years now. So, I think we should start pushing too.

I don't know what to do about fingerprinting. Personally, I'm dubious it's a problem that we could reasonably solve even if were to start all over with the Web. And I feel it's intractable with the Web as it is today. However, I also view that as a very different problem from a security perspective.

My big security concern is the ambient permission leakage that comes from allowing third-party cookies. So, I think there's a big value in solving that problem on its own, independent of user tracking (via cookies or fingerprinting) as a privacy issue.

I agree. I suspect Dominic/privacy agrees too.

-mike

On Tue, Aug 30, 2016 at 3:17 AM, Mike West <mkwst@google.com> wrote:

We didn't do things like https://docs.google.com/document/d/1tFLIeYmE8MR-m79MLSmJ_mHDHNQLn7yYo9aDBslKIVs/edit

or https://docs.google.com/document/d/1hK4nB3lZGCtII_r_tIPg4xPMmDr6Ahh9IL5veAccsrg/edit in the past for the two reasons that Jochen notes: fingerprinting, and identity providers.

Identity providers are solvable in some way via better UI for users or intelligent decisions the browser makes about when to allow cookies and when to block them ("Hey, you've been to this site at the top-level 100 times in the last week. Maybe you like it?").

Fingerprinting is harder. There's nothing we can technically do to prevent it, and we haven't been successful at creating a technical/regulatory framework in which to successfully ostracize it.

That said, based on some comments they've made in WebAppSec, Safari seems to be doing things to tighten their behavior in this area. I think it's something we should think about again. +battre from Privacy.

-mike

-mike

On Mon, Aug 22, 2016 at 1:54 PM, Jochen Eisinger <eisinger@google.com> wrote:
The other big use case are ID providers, i.e., you'll need to whitelist [google.com](https://www.google.com) to use teams.googleplex.com

In order to be able to [REDACTED]

We also need a better story for fingerprinting, as this will just push (non-IBA) ad networks into using fingerprinting instead of cookies.

On Tue, Aug 9, 2016 at 3:24 AM Joel Weinberger <jww@google.com> wrote:
My ignorance is astounding, but I assume third-party cookies are almost exclusively used by ad folks these days, yes? If so, should we bring Ojan and the Magnolia folks in on this?

On Fri, Aug 5, 2016 at 11:27 AM Artur Janc <aaj@google.com> wrote:
+sroettger

On Fri, Aug 5, 2016 at 11:18 AM, Justin Schuh <jschuh@google.com> wrote:
Here's the Blackhat presentation:
<https://www.blackhat.com/docs/us-16/materials/us-16-VanGoethem-HEIST-HTTP-Encrypted-Information-Can-Be-Stolen-Through-TCP-Windows-wp.pdf>

The tl;dr is that third-party cookie blocking would prevent HEIST from being able to steal sensitive content. I realize that this is subject is fraught with peril, but maybe it's time to take another crack at a [REDACTED]?

—
You received this message because you are subscribed to the Google Groups "chrome-security-owp" group.

To unsubscribe from this group and stop receiving emails from it, send an email to chrome-security-owp+unsubscribe@google.com.

To post to this group, send email to chrome-security-owp@google.com.

To view this discussion on the web visit <https://groups.google.com/a/google.com/d/msgid/chrome->

security-

owp/CAObUUC_j2SkZnYxLt5dw4vdRLxuPTZuMdM0s8ucdFkWrj7cRSw%40mail.gmail.com.

--

You received this message because you are subscribed to the Google Groups "chrome-security-owp" group.

To unsubscribe from this group and stop receiving emails from it, send an email to chrome-security-owp+unsubscribe@google.com.

To post to this group, send email to chrome-security-owp@google.com.

To view this discussion on the web visit <https://groups.google.com/a/google.com/d/msgid/chrome-security-owp/CAPYVjq%2BZRCAGxxwjNRSyeZei-9Mg9x-iWphjznmnNEV3WT-tw%40mail.gmail.com>.

--

You received this message because you are subscribed to the Google Groups "chrome-security-owp" group.

To unsubscribe from this group and stop receiving emails from it, send an email to chrome-security-owp+unsubscribe@google.com.

To post to this group, send email to chrome-security-owp@google.com.

To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/chrome-security-owp/CAHQV2K%3De7M6ZrZ3vy4R-FJts950M_gJVTB4c70_e1fm%2B4PC%3DrA%40mail.gmail.com.

--

You received this message because you are subscribed to the Google Groups "chrome-security-owp" group.

To unsubscribe from this group and stop receiving emails from it, send an email to chrome-security-owp+unsubscribe@google.com.

To post to this group, send email to chrome-security-owp@google.com.

To view this discussion on the web visit <https://groups.google.com/a/google.com/d/msgid/chrome-security-owp/CAKXHy%3DeVyk5S3ix-unmMFd-2SZyfiL0oh17KHcOV2yzQ4-xfw%40mail.gmail.com>.

EXHIBIT 36

Redacted Version of Document
Sought to be Sealed



Google Analytics: Starting Conversation

Last updated: November - 2020

Confidential • Proprietary

Agenda

1. Mission, Objectives, Key Metrics
2. Product Segmentation, Customers, Personas, User Clusters
3. Understanding the Product
4. The Industry Landscape
5. Pricing & Commercialization
6. Gold History
7. Architecture (Eng deep-dive to follow!)

Google

Confidential + Proprietary

Mission, Objectives, Key Metrics

Google

Confidential + Proprietary

Proprietary + Confidential

Our Mission

Be the privacy centric, intelligent, and actionable analytics system of record for large and small businesses.

Understanding the customer journey

Delivering intelligent insights

Empowering actionability

Google

Value to Google

#1

Protect and grow Google media spend

Influence strategic budgets and grow Google's digital share via better insights and integrations for customers.

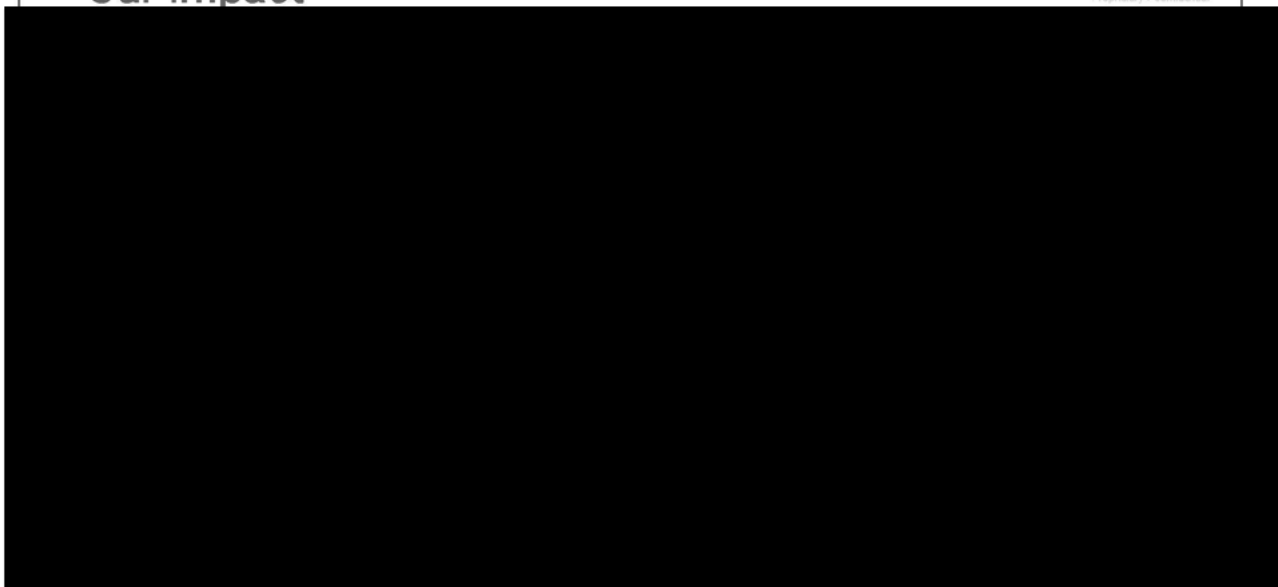


- We have a paid business because it is necessary to capture & influence Google's largest & most sophisticated customers (some customers will not adopt our product without a price tag, sales, services, SLAs, and enterprise capabilities)
- Our value also includes being: a key catalyst in driving better overall user experiences for the internet.

Google

Our impact

Proprietary + Confidential



Google

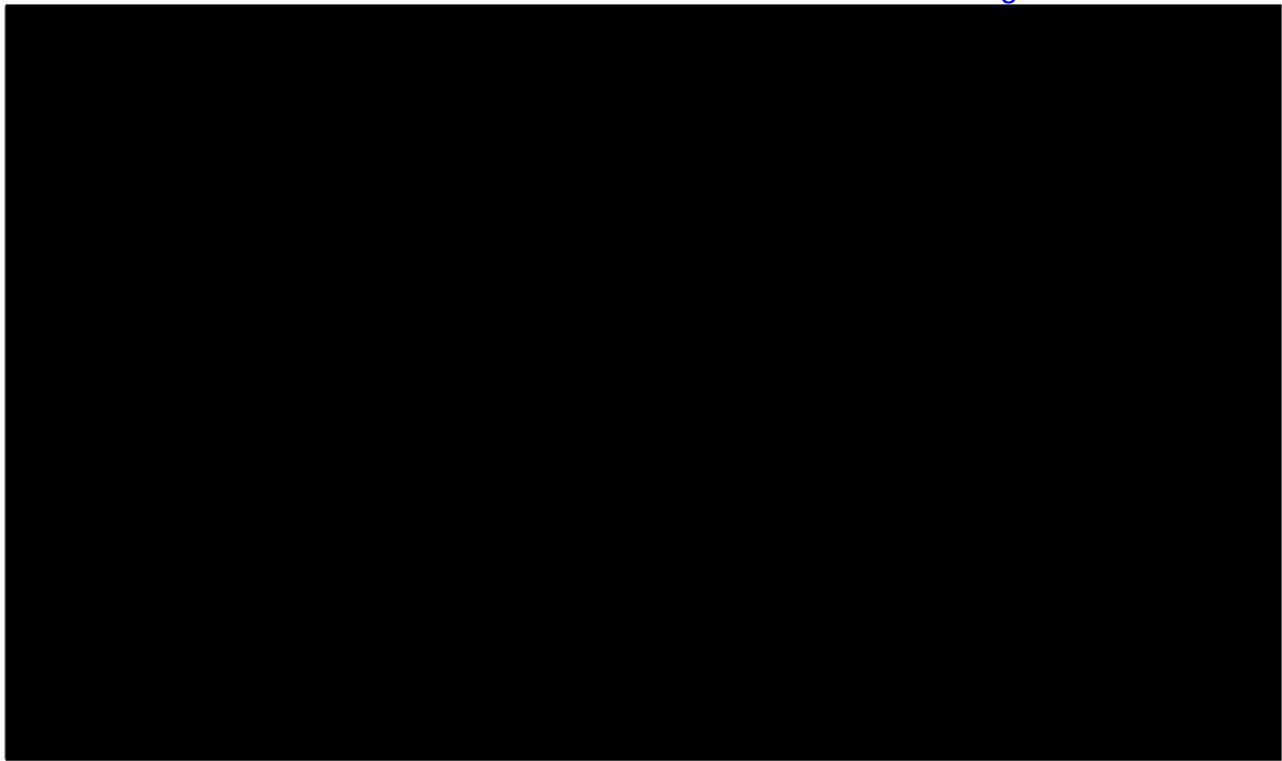


EXHIBIT 37
Redacted in its
Entirety

EXHIBIT 38
Redacted in its
Entirety

EXHIBIT 39
Redacted in its
Entirety

EXHIBIT 40
Redacted in its
Entirety

EXHIBIT 41
Redacted in its
Entirety

EXHIBIT 42
Redacted in its
Entirety

EXHIBIT 43

Unredacted Version of Document
Sought to be Sealed

CONFIDENTIAL

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

CHASOM BROWN, WILLIAM BYATT,
JEREMY DAVIS, CHRISTOPHER
CASTILLO, and MONIQUE TRUJILLO,
individually and on behalf of all similarly
situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 5:20-cv-03664-LHK

**DEFENDANT GOOGLE LLC'S OBJECTIONS AND RESPONSES TO PLAINTIFFS'
8TH SET OF INTERROGATORIES (NOS. 30-33)**

Pursuant to Federal Rule of Civil Procedure 33, Defendant Google LLC ("Google") hereby responds and objects to Plaintiffs' Interrogatories, Set 8 (Nos. 30-33). These objections and responses are made solely for the purpose of and in relation to this action. In addition, the objections and responses set forth in this document are based on Google's knowledge, investigations, and analysis to date. As discovery proceeds, Google may become aware of additional facts or evidence and its analysis of the case may change. Google reserves all rights to supplement and amend its objections and responses accordingly.

GENERAL OBJECTIONS

1. Google objects to Plaintiffs' definition of "GOOGLE," "YOU," and "YOUR" as encompassing "any of its directors, officers, consultants, agents, representatives, predecessors in interest, subsidiaries, assignees, licensees, employees, attorneys and any other persons acting on GOOGLE LLC'S behalf, including contractors," as well as "purporting to act on" Google's behalf. Google further objects to these definitions to the extent that it seeks to require Google to produce or otherwise analyze any document or other information that is not within the possession, custody, or

CONFIDENTIAL

1 control of Google. Google further objects to these definitions to the extent that it purports to impute
2 knowledge of unspecified or unknown parties or persons to Google. Google further objects to these
3 definitions as overly broad, vague, and ambiguous to the extent they purport to include entities other
4 than Google, which is the only named defendant in the present action. Google further objects to
5 these definitions and instruction to the extent that they include Google's attorneys and, therefore,
6 cause interrogatories using "Google" to improperly seek information protected by the attorney-client
7 privilege, the work product doctrine, the common interest privilege and/or any other applicable
8 privileges or immunities.
9

10 2. Google objects to Plaintiffs' definitions of "ALL," "INCLUDE," "INCLUDING,"
11 "CONCERNING," and "RELATING TO" to the extent that they propose to alter the plain meaning
12 or scope of any specific interrogatory and to the extent that such alteration renders the interrogatory
13 vague, ambiguous, and overbroad.
14

15 3. Google objects to Plaintiffs' definition of INSTANCES as vague, ambiguous and
16 overly broad.

17 4. Google objects to Plaintiffs' Definitions, Instructions, and interrogatories to the
18 extent they seek information and/or records that are not reasonably accessible and whose inclusion
19 is not proportional to the needs of the case.
20

21 5. Google objects to the interrogatories to the extent that they seek information shielded
22 from disclosure by the attorney-client privilege, the work-product doctrine, the settlement privilege
23 and/or any other applicable privilege or protection from discovery.

24 6. Google objects to Plaintiffs' Definitions, Instructions, and interrogatories to the
25 extent they conflict with or encompass information and/or records falling outside the scope of
26 discovery under the Federal Rules of Civil Procedure, the local rules of the Northern District of
27 California, or any discovery orders governing this case.
28

CONFIDENTIAL

1 7. Google's responses to these interrogatories are hereby made without waiving or
2 intending to waive, but rather, to the contrary, by preserving and intending to preserve:

- 3 a. All questions as to the competence, relevance, proportionality, materiality,
4 and admissibility as evidence for any purpose of the information or
5 documents, or the subject matter thereof, in any aspect of this action or any
6 other court action or judicial or administrative proceeding or investigation;
7
8 b. The right to object on any ground to the use of any such information or
9 documents, or the subject matter thereof, in any aspect of this action or any
10 other court action or judicial or administrative proceeding or investigation;
11
12 c. The right to object at any time in connection with any further response to
13 these or any other interrogatories; and
14
15 d. The right at any time to supplement its responses.

16 8. Google anticipates that future discovery, independent investigation, or analysis will
17 supply additional facts and add meaning to known facts, as well as establish new factual conclusions
18 and legal contentions, all of which may lead to additions to, changes in, and variations from the
19 responses set forth herein. Google reserves the right to modify, supplement, withdraw, or otherwise
20 alter its responses to these interrogatories in accordance with the Federal Rules of Civil Procedure,
21 the local rules of the Northern District of California, or any discovery orders governing this case.

22 **OBJECTIONS AND RESPONSES TO SPECIFIC INTERROGATORIES**

23 Subject to the foregoing objections, Google objects and responds to Plaintiffs' interrogatories
24 as follows:

CONFIDENTIAL

INTERROGATORY NO. 30:

Please explain all differences regarding how browsing data is sent from users' devices to Google when (1) a user visits a website that uses Google Ad Manager but not Google AdSense compared with (2) a user visits a website that uses Google AdSense but not Google Ad Manager.

RESPONSE TO INTERROGATORY NO. 30:

Google incorporates its General Objections as if set forth fully herein. Google further objects to this interrogatory as overbroad and unduly burdensome on the grounds that Google AdSense is not tied to Plaintiff's class definition. *See* Dkt. 136-1 (Second Amended Complaint ("SAC")) ¶ 192. Google further objects to this interrogatory as vague and ambiguous as to the meaning of the terms "browsing data" and "sent from users' devices to Google." Google will assume for purposes of its response that "browsing data...sent from users' devices to Google" means data generated when users visit third-party websites that use Google Ad Manager or Google AdSense while not logged into their Google Account. Google further objects to this interrogatory to the extent it seeks information related to non-Chrome browsers, which may have unique browser features that impact data collection by Google Ad Manager and Google AdSense. Google further objects to this interrogatory as overbroad and unduly burdensome because it seeks a description of "all" differences between data received by websites using Ad Manager or AdSense.

Subject to and without waiving the foregoing objections, Google responds as follows:

Google Ad Manager will not receive data related to a user's visit to a specific website unless Ad Manager scripts have been installed in the website's HTML code. Similarly, Google AdSense will not receive data related to a user's visit to a specific website unless AdSense scripts have been installed in the website's HTML code. The Ad Manager scripts are different from the AdSense scripts, but each may be viewed by any Chrome user by visiting the webpage using Google Ad Manager (or AdSense) and clicking on "View," "Developer," "Developer Tools," "Sources." The

CONFIDENTIAL

1 data sent to Google Ad Manager and Google AdSense depends on the functionality defined in the
2 respective scripts. The data sent to Google Ad Manager will differ from the data sent to Google
3 AdSense in a number of respects, due to differences between the two products and the respective
4 APIs they provide to publishers, which are described in publicly-available documentation. *See, e.g.,*
5 <https://developers.google.com/publisher-tag/guides/get-started>;
6 <https://support.google.com/adsense/answer/9274634>.

7
8 The data sent to Google Ad Manager or Google AdSense also depends on a number of other
9 factors. When a user (in any browser) visits a website that uses Google Ad Manager or AdSense,
10 Google Ad Manager or AdSense may receive: (1) cookies that specific Google domains previously
11 set on the user's browser; (2) the HTTP request sent by the user's browser, including the hostname,
12 browser type, and language, and depending on the browser used, Java support, Flash support, and
13 screen resolution; (3) the URL of the website making the ad request to Google Ad Manager or
14 AdSense, and/or the referrer URL; (4) the IP address assigned to the device on which the browser
15 is running; (5) the request for an ad to be served on a non-Google website and the ad slot to be filled;
16 (6) event data such as impressions or clicks; and (7) if the user is in Chrome and a mode other than
17 Incognito, the browser's X-Client-Data Header. The X-Client-Data Header may also be empty even
18 when the browser is not in Incognito mode, including: (i) a new browser instance (ii) the browser
19 has not been used for 30 days or more; (iii) the Chrome server sends too many variation IDs to the
20 Chrome browser thereby causing the Chrome browser to delete the header to keep it from becoming
21 too large; and (iv) a firewall prevents Chrome from receiving the variation IDs that are used to
22 populate the X-Client-Data Header.

23
24
25 Whether Google in fact receives these categories of data depends on numerous factors,
26 including (1) features and settings enabled by the user in Chrome or in the user's Google Account
27 settings and (2) use of third-party software by the user. For example, Chrome's cookie settings,
28

CONFIDENTIAL

1 which are accessible via a drop-down menu or by navigating to chrome://settings/cookies, include
2 an option to “block all cookies.” When the user enables this feature, Chrome prevents websites,
3 Google Ad Manager and AdSense from setting or receiving any cookies. If all cookies are blocked
4 in this manner, the Chrome browser will not send any cookies to Google Ad Manager or AdSense.
5 Chrome’s settings also include an option to “block third-party cookies.” When the user enables this
6 feature, Chrome does not set or transmit to Google Ad Manager or AdSense any third-party cookies,
7 including advertising cookies. Similarly, enabling “clear cookies and site data when you close all
8 windows” in Chrome settings means that cookies do not persist across browsing sessions and
9 Google Ad Manager and AdSense will not receive any cookies set in a prior session.
10

11 As another example, Chrome’s JavaScript settings, which are accessible via a drop-down
12 menu or by navigating to chrome://settings/content/javascript, include the following option: “Don’t
13 allow sites to use Javascript.” When a user selects “Don’t allow sites to use JavaScript,” Chrome
14 prevents websites from using JavaScript, including Google Ad Manager and AdSense tags based on
15 JavaScript. As a result, if JavaScript is disabled in this manner, the Google Ad Manager or AdSense
16 JavaScript tag will not be able to send information to Google Ad Manager or AdSense when a
17 Chrome user visits a website that uses Google Ad Manager or AdSense.
18

19 There are also multiple ad-blocking extensions available on the Chrome Web Store that,
20 when installed, can be configured to block Chrome from sending ad requests. Popular examples of
21 those extensions are Adblock and Adblock Plus. When installed by a user, these ad-blocking
22 extensions may, depending on their configuration, prevent Chrome from sending ad requests to
23 Google Ad Manager or AdSense. There are also multiple standalone (not browser extension/plug-
24 in) ad blocker programs that are designed to provide the same ad-blocking functionality. Popular
25 examples of those programs are AdGuard and AdLock. When installed by a user, these ad-blocking
26 programs may, depending on their configuration, prevent Chrome from sending any ad requests to
27
28

CONFIDENTIAL

1 Google Ad Manager or AdSense, thus preventing Google Ad Manager or AdSense from receiving
2 any of the information described above.

3 If Chrome is used in Incognito mode, Chrome will not send the X-Client-Data Header to
4 doubleclick.com or any other domain used by Google Ad Manager or AdSense. Furthermore, when
5 a user activates Incognito mode, Chrome will create a new cookie jar that only stores first-party
6 cookies and third-party cookies if not blocked (the default setting is for third-party cookies to be
7 blocked in Incognito mode) for the duration of that Incognito session, and those cookies are deleted
8 when the Incognito session ends. Because Chrome creates a new cookie jar for the Incognito session,
9 Google Ad Manager and AdSense will not receive any cookie values set in a prior session. Similar
10 to Incognito mode, when a user activates Guest mode, Chrome will create a new cookie jar that only
11 stores cookies for the duration of that Guest mode session, and those cookies are deleted when the
12 Guest mode session ends. Because Chrome creates a new cookie jar for the Guest mode session,
13 Google Ad Manager and AdSense will not receive any cookies set in a prior session.
14
15

16 There are also a number of third-party privacy programs and features that users can employ
17 that affect whether Google Ad Manager or AdSense receives the data at issue, including proxy
18 servers and VPNs, firewalls, ad blockers, and opt-out features. For example, if a Chrome user or
19 their network administrator employs a proxy server or VPN (Virtual Private Network) that masks
20 the sending device's IP address, then Google Ad Manager or AdSense would not receive the user's
21 real IP address. Instead, Google Ad Manager or AdSense would receive only the IP address assigned
22 by the VPN or proxy server. And if a Chrome user or their network administrator employs a firewall
23 that is configured to allow traffic only to specific domains (not including domains associated with
24 Google Ad Manager or AdSense), or to prevent traffic to specific domains (including domains
25 associated with Google Ad Manager or AdSense), then any transmissions that the Chrome browser
26 attempts to send to Google Ad Manager or AdSense will be blocked by the firewall. Firewalls can
27
28

CONFIDENTIAL

1 also prevent Chrome from receiving the variation IDs that are used to populate the X-Client-Data
2 Header.

3 When a user (in any browser) visits a website that uses Google AdSense, Google AdSense
4 may receive many of the same types of data described above for Google Ad Manager (subject to the
5 same factors described above). However, Google AdSense will not receive certain items of data
6 that are only relevant to Google Ad Manager. For example, as described in publicly available
7 documentation, Google Ad Manager allows publishers to set a publisher-provided identifier (PPID).
8 See <https://support.google.com/admanager/answer/2880055>. Google AdSense does not provide this
9 feature, so when a user visits a website that uses Google AdSense, the browser would not send a
10 PPID value to Google AdSense.
11

INTERROGATORY NO. 31:

12 Please explain the basis for Google's determination that "false positives" for Chrome
13 Incognito browsing detection in log-based analyses "range from [REDACTED] (GOOG-BRWN-
14 00204687), including by identifying documents and individuals tied to this determination.
15
16

RESPONSE TO INTERROGATORY NO. 31:

17 Google incorporates its General Objections as if set forth fully herein. Google further objects
18 to this interrogatory to the extent it mischaracterizes a draft document prepared by individual Google
19 employees as "Google's determinations" regarding "'false positives' for Chrome Incognito
20 browsing detection." Google further objects to this interrogatory as vague and ambiguous as to the
21 meaning of the terms "Chrome Incognito browsing detection," "log-based analyses," and "tied to
22 this determination."
23
24

25 Subject to and without waiving the foregoing objections, Google responds as follows:

26 The estimated "false positives to identify Chrome traffic" ranging from "[REDACTED]" referenced
27 at GOOG-BRWN-00204684 at -87 was based on differences observed between certain statistics
28 collected from multiple independent sources, including data available to Chrome engineers and data